情報セキュリティ対策個人マニュアル

あなたのパソコンを守るために

Red Hat Linux 8.0 編

平成15年3月

北海道大学

利用者向け情報セキュリティ対策マニュアルの作成および方法論に関する調査研究グループ

Version 1.1

目次

はじめに

北海道大学にはじめて，今日のインターネットの前身といえる JUNET のための直通電話回線が，文学部行動科学科 (現在の人文科学科行動システム科学講座) に引かれたのは 1986 年のことであり，その後，1988 年に工学部情報工学科へ移設されました．一日に数回，自動的に東京から電話がかかってきて，それにより世界中にメールを出すことができるだけで大きな喜びを感じられる時代でした．1990 年には学術情報センター (現在，国立情報学研究所) 主体の専用回線による大型計算機センターと東京大学，京都大学等との相互接続配送に移行しました．1989 年のキャンパスネットワーク HINES(ハイネス) の稼働に伴って利用者層を広げていきましたが，1988〜1993 年までは工学研究科情報工学専攻 (現在，システム情報工学専攻) の数名の有志，その後現在に至っては大型計算機センターに代表される多くのボランティアや教職員の努力により，現在の状況を向かえています．その間，インターネットは世界的に急激な発展を遂げ，一般家庭でも気楽に利用できるようになってきました．10 数年前から比べると夢のような世界が出現しています．隣の机の上にあるパソコンも，地球の裏側にあるスーパーコンピュータも同じ手順でつながっています．

しかし，反面やっかいなことも起きてきました．学内のほとんど全てのコンピュータには，ネットワークを介して，毎日，なんらかの不正な攻撃がなされていると考えられます．また，学内外からコンピュータウイルスがついた電子メールが次から次へと届いています．いわゆるホームページを見ただけでウィルスに感染するような場合もあります．本学のネットワークの大本である大型計算機センターでも多くの対策をとっていますが，管理元での防御だけでは限界があります．そこでまずは，あなたの机の上にあるパソコンに対して，できる限りのセキュリティ対策をして頂きたいと思います．対策が不十分ですと，あなたの貴重なデータが消えたり，改変されたり，流出する可能性があります．さらに，攻撃の「踏み台」にされて，大学内外の多くのコンピュータに悪影響を与える場合もあります．

本セキュリティマニュアルは，本学のネットワークである HINES に接続するパソコンなどが，安全に利用できるための最低限の方法についてまとめたものです．鍵をかけていても，泥棒に入られる可能性をゼロにすることはできません．しかし，鍵をかけない場合に比べると，その可能性は非常に少なくなります．そこで，情報関係の専門家ではない方が市販のパソコンを HINES に接続することを想定し，注意すべき事項をまとめました．残念ながら，100 %安全な対策であると主張することはできませんが，必要最低限の対策です．学内外のセキュリティに関係する事情も急激に変化しております．平成 15 年度か

ら本学に設置される予定の情報基盤センターを中心として，セキュリティ対策の情報が発信されると思われますのでそれらにも注意を払ってより安全なコンピュータ環境を作って下さい．本セキュリティマニュアルには，Windows 2000 編，Windows XP 編，Red Hat Linux 8.0 編，Vine Linux 2.6 編の 4 分冊があります．それぞれ独立して読めるようになっておりますので，必要なものをお使い下さい．

平成 15 年 3 月 31 日

注意：本マニュアルにある製品名などは，各社の登録商標です．北海道大学および本マニュアル作成メンバーは，特定のソフトウェアの推薦や動作保証をするものではありません．本マニュアルの利用により，セキュリティが向上することを目指しておりますが，本マニュアルに記載された設定等を施しても事故が起きる可能性をなくすことはできません．本マニュアルに記載された対策を施した後に事故が発生しても，責任を負いかねることなど，本マニュアルの性格をご理解頂いた上で，御活用頂けますよう，お願い申し上げます．

利用上の注意

このマニュアルは,「購入したコンピュータに Linux を入れ，サーバとしてではなくクライアントとして利用する目的で HINES につなぐ．さてセキュリティ対策として最低限何をしなければならないか」という問いに対する回答として作られています．そのためこのマニュアルでは Linux の初歩的な使い方や技術用語の解説は，最小限に抑えられました．このマニュアルは，初心者が Linux を使えるようになるマニュアルではなく，初心者でもこの通りに作業を行えば一通りのセキュリティ対策ができる，というものを目指しています.

ある程度の解説をつけましたが，十分であるとは言い難い内容量ですので，分からない用語などは適宜，初心者向けの Linux 入門書などを参照されることをお勧めします．また内容に関するご質問やご意見は学内ニュースグループである hu.misc や，HINES セキュリティマニュアル Linux 対策マニュアル作成グループのウェブサイト（http://genki01.cc.hokudai.ac.jp/project/security/）にある掲示板などでも受け付けております．ここで得られた修正案を元に，改訂版を随時アップロードしておりますので，最新版にアクセスしたい場合は上記のウェブサイトをご覧になる事をお勧めします.

必要最低限の意識

Linux であるとか，Windows であるに関わらず，何らかの手段を用いてセキュリティ対策を行う以前に存在する，コンピュータを利用するにあたって必ずもっていなければいけない意識について述べます.

1. **パスワードの管理**
   安易なパスワードをつけると，それは実に容易く解読され盗まれてしまうという事を知るべきです．またパスワードは他人と共有してはいけませんし，他人に教えることもしてはいけません．また，付箋紙に書いてディスプレイに貼り付けて置くことは，ボンネットの上に鍵を置いて車を駐車するに等しい行為です．これらのパスワードに関する注意事項は，理学部の「物理実験 I：情報実験プロジェクト」のウェブサイトに詳しいです. *[1]

*[1] http://www.ep.sci.hokudai.ac.jp/ inex/y2002/1018/1018.2.html#passwdsec

2. **ログインしたまま席を離れない**
   ログインして，様々な操作が可能な状況のまま，席を立たないで下さい．席を離れる間が短くてもロックをするべきです．事実，トイレに行くため席を離れたその短い時間に，電子メールクライアントを悪用され，とある組織に対する脅迫メールを出されてしまったという事件もかつてありました．また，そのコンピュータの中に入っている様々な個人情報を盗むということも非常に簡単に出来てしまいます．

3. BIOS **にパスワードをかける**
   最近のコンピュータでは BIOS の起動時にパスワードの入力を求めることが出来ます．このパスワードは設定するべきでしょう．ほとんどどんな OS でもそうですが，OS が起動する前に様々な手段を講じられてクラッキングされてしまうと，どれほど強固なセキュリティ対策を施していようと，全くその対策は効果を発揮できず無意味になります．自分以外の人間がコンピュータを起動することをできないようにするべきです．これは決して極端な話ではありません．

各種情報源

セキュリティ対策に必要な情報は絶えず変化していきます．新聞を読むような感覚で，以下にある情報に必ず目を通すようにしましょう．

- Red Hat Linux 8.0 **のサポート情報**
  http://www.jp.redhat.com/support/8.0/

- Red Hat Linux 8.0 **パッケージの更新情報・エラータ**
  http://www.jp.redhat.com/support/errata/rh80/

- **日本の** Linux **情報**
  http://www.linux.or.jp/

- JPCERT/CC
  http://www.jpcert.or.jp/

- IPA **情報処理振興事業協会**
  http://www.ipa.go.jp/

- **セキュリティホール** memo
  http://www.st.ryukoku.ac.jp/ kjm/security/memo/

- HINES **ホームページ**
  http://www.hokudai.ac.jp/hines/

凡例

また，本マニュアルでは以下のような表現を用います．

↵	Enter キーを打鍵する．
`[hoge@Linux00 hoge]$`	計算機名 Linux00 で，一般ユーザ hoge が hoge というディレクトリにいる場合の プロンプト表示
`[root@Linux00 hoge]#`	計算機名 Linux00 で，root が hoge というディレクトリにいる場合の プロンプト表示

第1章

北海道大学内部におけるコンピュータセキュリティについて

本マニュアルはいわゆる「コンピュータセキュリティ」を対象としていますが，昨今のインターネットの普及などと相まって，非常に漠然とした形でしか理解されていない向きもあると思います．そこで，具体的な方法論に入る前に，学内における「コンピュータセキュリティ」について，本マニュアルに記載された内容やノウハウの必要性をご理解いただけるよう，概説を試みたいと思います．

1.1 コンピュータセキュリティの必要性

一般にセキュリティを論じる際，はじめに思い浮かぶのは，自分のコンピュータの安全性だと思います．確かにその通りですが，それ以上に気にかけて頂きたいのは，「人に迷惑をかけないための安全性」です．

たとえば，最近大規模に被害を生じたコンピュータウイルスの多くは，侵入に成功したコンピュータに保存されている電子メールからメールアドレスを適当に拾い，その拾ったアドレスを名乗って別のアドレスへ自分を送り出す性質を持っています．また，本来ならば接続できない機材に接続を試みたり，一時的に大量のデータもしくは大量の接続要求を送って，コンピュータの動作を著しく遅くするような不当行為は，多くの場合，本来の接続先を探られないよう，不正にアクセスして成功した機材から行われます．

どちらの場合も，侵入を防げれば被害の拡大を抑えることができるのですが，なかなかそうはいかないようです．ただ，その後，たとえばコンピュータウイルスに自分のメールアドレスを語られ，全く身に覚えがないのにウイルス送信者として知己の方々から責められたり，自分がしたわけでもないのに不正アクセス者としてクレームを受けたりと，１度とばっちりを受けると後々まで禍根を残します．

「自分のコンピュータを守る」ことは「他人のコンピュータに迷惑をかけない」ことと同じであるとともに，むしろ他人に迷惑をかけないために，自分のコンピュータの安全性をしっかりと確かめておくべきなのです．

1.2 実際の「コンピュータセキュリティ」対象

上にも書きましたが，現在，ネットワーク接続のあるコンピュータで「セキュリティ対策」といえば，以下の 2 種類に集約されると思います．

1. コンピュータウイルス対策
2. 不正アクセス，不正利用対策

コンピュータウイルスは，以前はフロッピーディスクであった感染経路がインターネットへとかわり，多くは電子メール閲覧やホームページ閲覧により感染します．伝播する速度もネットワークの広域化, 高速化と相まって飛躍的に向上（？）しています．メール閲覧に関しては Microsoft Outlook(Express 含む)，ホームページ閲覧では Internet Explorer と，ターゲットとしては Microsoft Windows が圧倒的なシェアを誇っています．

一方，不正アクセスや不正利用は，その性格上，サーバと呼ばれるような，24 時間稼働しているコンピュータがターゲットとなっています．特に Linux に代表されるような，一般的なパーソナルコンピュータ上でも動作するようになった UNIX 系，もしくはそれに類する環境への攻撃が多いようです．ただし，最近は Windows などでも動作するホームページサーバープログラムや Windows Server などがあり，これらも標的となっています．

1.3 包括的管理の限界

HINES の管理運用は，本マニュアル作成時点では大型計算機センターが行っており，メールに含まれたウイルスの除去や，不正アクセスの原因となりかねない外部からの接続要求を拒否するよう，外部との接続点で様々な対策が施されています．

「ならば，なにも私が自分で対策など…それはしかるべき部署の仕事ではないのか？」という疑問を潜在的にでも持たれる方,「自分は専門家ではないので，そんなことをする気にはなれない」「私はそんなことをするために大学に奉職しているのではない」とご自身の立場を主張される方もおられると聞きます．

しかし，これらは大きな誤りです．考えてもみてください．いかに専門外といえども，ご自身の研究室のドアの鍵を開け放たれたままにされる方はさすがにおられないと思います．インターネットに接続されているコンピュータは，何も対策を施さなければ，まさに「鍵を開け放たれたままの部屋」です．しかも現実空間の部屋の場合，被害があってもほとんどの場合，本人だけが責任をとれば済みますが，先に述べた通り，コンピュータへの被害は他人に迷惑をかける可能性が極めて高いのです．

加えて，根本的な誤解をされる方が多いので，はっきりと書いておきたいのですが，この節の最初の段落をもう 1 度よく読んでください．

「外部との接続点で」

とあります．すなわち，学内相互の通信については，原則として対策が施されていない

のです．本学のような規模になりますと，内部での被害も非常に大きなものとなります．また，これも前の方に書きましたが数千台あるコンピュータをすべて，大型計算機センターで常時監視することは現実的に不可能ですし，たとえば持ち込まれた CD-ROM などにウイルスが含まれているなど，物理的な経路まではチェックのしようもありません．

特定部署による包括的管理では不十分であり，いわば水際作戦とでもいうべき，個々人レベルでの各種対策が必要であることをぜひご理解ください．

1.4　導入後のケア

ここまで読んで頂いて，個人レベルでのセキュリティ対策の必要性をご理解頂けたと思います．次章以下では，Windows および Linux を例にとり，安全策について最低限の説明を行っていますので，ぜひこれに沿って対策を施してください．

ただし，書かれた内容に沿って導入しただけでは終わりません．その後もずっと手をかけて頂く必要があります．

コンピュータウイルスソフトウェアのミッションはつまるところ，これまでに報告されたウイルスの感染パターンを記憶しておき，一致したものを排除することにあります．ご存じのとおり，コンピュータウイルスは日々新種が発見されます．つまり感染パターンも日々増えています．

例に挙げた対策ソフトウェアは，導入時から 1 年間，最新の感染パターンをインターネット経由で入手，更新できる権利がついています．特に最近のソフトウェアは自動的に更新を促すようになっていますので，これをぜひ活用し，常に最新のデータを得てから利用するようにしてください．

また，不正アクセスの手がかりとなるのは，Windows や Linux に潜在的に残っていた不具合です．これを直すために，Windows では Windows Update という機構が備わっていますので，上に書いたウイルスパターン同様，原則として常に更新する方がよいでしょう．Linux などの場合は，主なホームページなど，インターネット経由で不具合と対応策が公開されます．Windows よりも対策を施すのは難しいと思いますが，特に不正アクセスについては Linux などでの被害の方が大きくなりがちですので，覚悟を決めて対応されることをおすすめします．

1.5　マニュアル記載以外の「安全性」への注意

本マニュアルで取り上げていない事項でも，安全性という観点から留意すべき点はあまたあります．たとえば「パスワード」の問題です．

メールを読み出す度に打つのは面倒だから，とメールソフトウェアにパスワードを記憶させている方が少なくないようですが，先に挙げたような部屋の例になぞらえれば，ドアの横に鍵をくくりつけているようなものではないでしょうか．特に最近では，コンピュータ上に記録されているパスワードファイルの内容を盗み出すウイルスさえあるようです．

また，パスワードを紙に記録されている方，何かの問い合わせをする際にパスワードを

メールに直接書かれる方などの例も聞きますが，いずれも絶対にやめてください．キャッシュカードの暗証番号になぞられていただければ，いかに危険な行為か，おわかりいただけると思います．

このほか，気にかけるべきこととしては，以下のようなものが考えられるでしょう．()内は留意すべきポイントです．詳細はまた別の機会に譲りたいと思います．

1. Web などでのフォームへの入力（入力内容を記録するブラウザ，入力先での管理の妥当性）
2. 暗号化されていないフォームデータの送信（不正盗聴の問題，相手側の情報管理姿勢）
3. 不用意な「掲示板」「チャット」の設置
   （利用プログラムの安全性の問題，「荒らし」への技術的措置能力の有無）

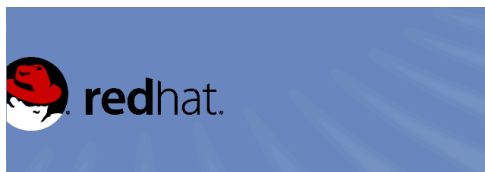
1.6 概説のおわりに

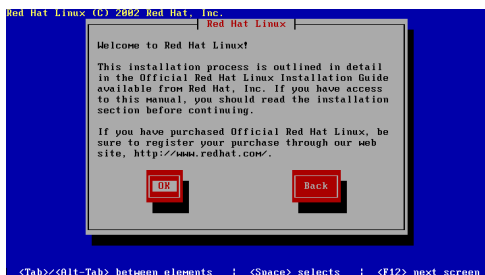
以上，書かれたことすべてに注意を払うには，かなりの労力が必要になると思います．しかし，だからといってそのままにしておいた場合，ことが起きて困るのは他の誰でもなく，被害を受けた本人です．

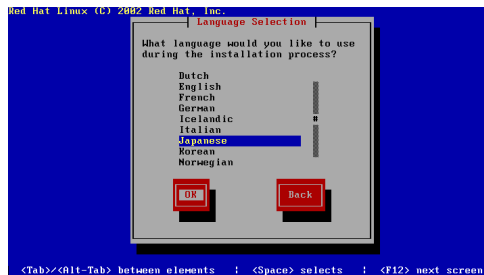
この機会にぜひ，自分のことは自分で守る，他人に迷惑をかけないためにも，自分の身の回りを整えることを習慣づけて頂くよう，お願いします．本マニュアルがその一助となるよう，祈念しております．

第 2 章

Red Hat Linux 8.0 のインストール手順

製品版 Red Hat Linux のインストールの手順を簡単に説明します．Red Hat Linux の CD をドライブに挿入して，マシンを起動してください．この説明は CD-ROM からの起動に対応したマシンのみを対象としている事をお許し下さい．CD-ROM からの起動に対応していない場合は起動フロッピーディスクを作成する必要があります．その説明はここでは割愛させて頂きます．

インストールモードの選択

グラフィカルモードかテキストモードの選択を行います．何も入力せずに Enter を押せばグラフィカルモードになります．テキストモードで行うには boot プロンプトに “text” と入力し，Enter キーを押してください．ビデオカードによってはグラフィカルモードで行えず，テキストモードでしか行えないことがあります．本マニュアルでは，テキストモードでの手順の説明をします．

ようこそ

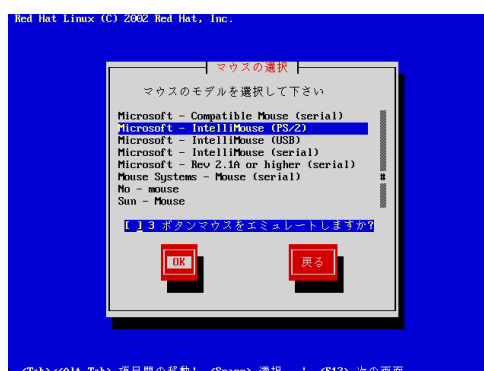
Red Hat Linux のインストールはここから始まります．[OK] を押して先に進みます．

インストールの使用言語

インストールで使用する言語として [Japanese] を選択します．自分の理解できる他の言語でも構いませんが，本マニュアルでは [Japanese] を選択した場合で以降の手順を説明していきます．言語を選択したら [OK] を押してください．

改めてようこそ

先ほどインストールのための言語を選択したので，ここから先は日本語でインストールを進めることができます．日本語画面で再びユーザ登録からはじまります．この画面では [OK] を選択します．

キーボードモデルの選択

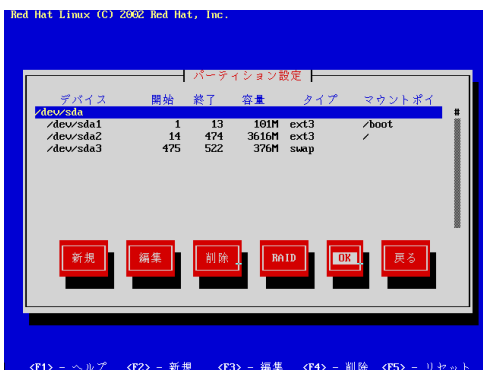
使用しているキーボードを指定します．日本語のキーボードをお使いなら [jp106] を選択してください．選択したら [OK] を押します．

マウスモデルの選択

使用しているマウスのモデルを選択します．2 ボタンマウスを使用しているのなら [3 ボタンマウスをエミュレートする] にチェックを入れると，2 ボタンマウスでも左右 2 つのボタンを同時に押すことで 3 ボタンマウスの中央のボタンを押すことに相当するよう設定できます．選択したら [OK] を押してください．

インストールの種類

インストールのタイプを目的に応じて選択してください．以降は [カスタム] を選択した場合で手順の説明を進めます．選択したら [OK] を押してください．

ディスクパーティション

ハードディスクの使用領域を分割します．ここでは簡便のために [自動パーティション設定] を選択することにします．もちろんパーティションに関する知識があれば，適切な分割を行う方が良いでしょう．

パーティションの設定

パーティションを希望に合わせて変更できます．変更し終わったら [OK] を選択してください．わからない場合はデフォルト設定のままで [OK] を押して構わないでしょう．

ブートローダの設定 (1)

使用するブートローダの設定です．[GRUB] か [LILO] あるいは [使用しない] のいずれかを選択します．ここでは [GRUB を使用] を選択することにしましょう．

ブートローダの設定 (2)

ここは特に設定する必要はないでしょう．設定が必要になる場合は後で設定を加えることも GRUB であれば可能です．ここはこのまま [OK] を選択しましょう．

ブートローダの設定 (3)

マシン起動時のセキュリティを考慮するのならブートローダのパスワードを決定します．ブートパスワードを設定する必要がないのならなにもせずにそのまま [OK] を押してください．

ブートローダの設定 (4)

他の OS とのデュアルブートを行う際はここで設定を行う必要があります．デフォルトで起動する OS を選択し [OK] を選択してください．コンピュータに Linux のみをインストールする場合はエントリがひとつしかありませんので，迷うこともありません．

ブートローダの設定 (5)

ブートローダのインストール場所を指定します．ここはマスタブートレコーダ (MBR) を選択した方が良いでしょう．場所を指定してから [OK] を押してください．

eth0 用ネットワークの設定

DHCP サーバがある場合は [boot/dhcp を使用] するにチェックを入れるだけで完了ですが，無い場合は IP アドレス，ネットマスク，デフォルトのゲートウェイ，DNS サーバを指定します．これらの情報が不明の場合はシステム管理者にお尋ね下さい．入力が正しいか確認したら [OK] を押します．

ホスト名の設定

今 OS のインストールを行っているマシンの名前を決めます．マシン名を入力したら [OK] を押してください．

ファイアウォール設定

ここではファイアウォールの設定を行えます．ここで設定しても，後から変更は可能ですので，インストール直後はセキュリティレベルを「高」に設定し，セキュリティアップデートを行った後に任意のセキュリティレベルに設定するのが良いかと思われます．選択したら [OK] で次へと進みます．

言語サポート

OS で使用する言語を選択します．[Japanese] を選択してください．他にも複数の言語を選択できます．選択したら [OK] を押してください．

標準の言語

[Japanese] を選択してください．選択したら [OK] を押してください．

タイムゾーンの選択

使用する地域に合わせて選択してください．日本で使うのであれば [アジア/東京] を選択します．選択したら [OK] を押してください．

root パスワードの設定

root(管理者) パスワードを設定します．上の欄にパスワードを入力し，確認のため下の欄に再度入力します．上下にパスワードを入力したら [OK] を押します．パスワードが上下正しいと次へ進みます．[OK] を押しても次へ進めないときは 2 つのパスワードが一致していないのでもう一度入力してください．

ユーザの追加

インストールが完了した時点でログインできるユーザアカウントを作成します．root アカウントはシステム管理のみに使用するものなので，通常は root 以外のユーザアカウントでログインします．ユーザのアカウント名，パスワードを 2 回，そのアカウントを持つユーザのフルネームを入力したら，[OK] を押します．

ユーザアカウントの設定

必要であればユーザアカウントは追加できます．さらに別のユーザアカウントを追加するときは [追加] を，次へ進むなら [OK] を選択してください．

ワークステーションデフォルト

[ソフトウェア選択をカスタマイズ] にチェックをいれて [OK] を押してください．

認証設定

セキュリティレベルを高めるため，[シャドウパスワードを使用] [MD5 パスワードを有効にする] にチェックを行ってください．以下の欄は環境に応じて記入しますが，NIS や LDAP サーバが用意されている場合はネットワーク管理者にお尋ね下さい．設定を行ったら [OK] を押しましょう．

パッケージグループの選択

個々のパッケージを選択することができますが，マニュアルの便宜上，ここでは全てインストールすることにしましょう．[Everything] を選択し，[OK] を押します．

インストール開始

インストール開始前に，インストールの記録を保存するかを聞かれます．[OK] を押します．

インストール中

インストールが終わるまでの残りの推定時間が表示されます．数分から数時間かかります．それまで先に進めることはできないのでしばらく待ちましょう．

ブートディスク作成

インストールが終わるとブートディスクを作成するかを問われます．何らかの理由でシステムが正常に起動しない場合，ブートディスクがあれば復旧の手助けとなるでしょう．作成したほうが便利なので空のフォーマットされたフロッピーディスクをドライブに挿入して [はい] を選択します．もちろん，ブートディスク作成をせずに進めることもできます．

ビデオカードの設定

X Window System で使用するためのビデオカードの指定です．デフォルト（自動的に検出された）表示で正しいはずですが，間違っていたり，未検出の場合は変更してください．ビデオカードの説明書などを参照して，正しく指定されているのを確認できたら [OK] を押します．

モニタの設定

使用しているモニタを一覧の中から選択します．自動的に検出されますが，検出されなかったり適当でない場合は自分でモニタの取扱説明書を読むなどして手動で編集すると良いでしょう．

X 設定のカスタマイズ

X Window System のための設定です．色数，解像度，ログイン画面の設定を行います．わからなかったらデフォルトのままにし，インストール後に変更してください．Windows を扱った経験がある人ならば [グラフィカル] のログイン画面のほうが馴染みやすいでしょう．決定したら [OK] で次に移ります．

インストール完了

この画面が出れば Red Hat 8.0 のインストールの完了です．CD をドライブから取りだし [OK] を押してください．

第 3 章

最低限の基本操作

Linux のような UNIX 系 OS は，Windows とは異なり，コマンドラインからの操作を多く要求されます．最低限の基本操作を修得する事が UNIX 系 OS を使いこなす要であると考え，ここでは各種コマンドなど，基本操作の説明をします．

3.1 基本操作

3.1.1 ログインする

1 台のマシンは，複数のアカウント (使用資格) を持つユーザによって使用されます．マシンにログインするためには，ユーザ名とパスワードを入力しなければなりません．

インストールで X の設定に成功し，グラフィカルログインを選択した場合，Linux を起動すると，GDM (GNOME Display Manager) によるログイン画面が表示されます．[ログイン名] と書かれたテキストボックスにユーザ名とパスワードを入力することでログインできるほか，この画面にある [セッション] などにより，後述する再起動や停止処理を行うことができます．

GUI でログインするのではなく，CUI によるコンソールログインも可能です．また，X の設定に失敗した人やグラフィカルログインを選択しなかった人は上記のような画面が出ませんので，コンソールログインせざるを得ません．また，グラフィカルログインを選択した人がテキストログインするためには，Ctrl-Alt-F1[*1]を押します．すると

```
Login:
```

と表示されますので，ユーザ名を入力します．次に，

```
Password:
```

と表示されますので，パスワードを入力してください．コンピュータにログインすると，プロンプトと呼ばれるコマンド入力待ち受け画面が表示されます．ここでコマンドを入力し Enter を押す事で，コマンドを実行することができます．

[*1] F1 以外でも，Ctrl-Alt と F1～F6 との組み合わせでコンソールに落ちることが出来ます．

3.1.2　ログアウトする

作業が終了しコンピュータの使用を終える時には，コンピュータからログアウトします．グラフィカルログインをして，例えば Red Hat Linux の標準デスクトップ環境である GNOME においてログアウトをしたい時は，画面左下の (Windows で言うならば，[スタート] メニューに相当する) 赤い帽子のボタンからログアウトを選んでください．この手順からでも後述する停止や再起動処理をすることができます．

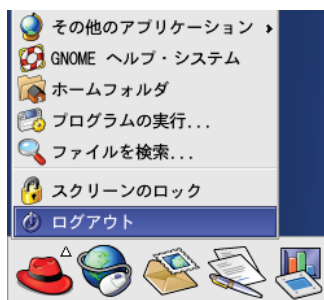



図 3.1: メニューアイコンからログアウトする

テキストログインしている場合はコマンドラインから logout と入力します．

```
[hoge@Linux00 hoge]$ logout ↵
```

3.1.3　sync，shutdown　システムの停止・再起動

コンピュータの電源を切る場合，あるいは再起動する場合には，その前にすべてのプロセスを順序正しく終了させるため，シャットダウン処理を行わなければいけません．前述のようにグラフィカルログインをしている場合は，GDM のログイン画面からこのシャットダウン処理を行うことができますが，ターミナルなどのコマンドライン上などからでもシステムの停止や再起動をすることが可能です．

コマンドライン上でシステムの停止処理を行うためには shutdown コマンド使います．また，シャットダウンする前には，安全のためにカーネルバッファの内容をはきだしてディスクに書き込む必要があるため sync コマンドを用ることが古くから言い伝えられてきましたが，Linux に入っている shutdown コマンドでは，この同期処理を行ってしまいますので，sync コマンドを実行する必要はありません．ですが，sync を三回実行してから shutdown するというおまじない的慣習を太古から受け継ぐのは (感情的には) 悪くない事だと思います．システムの停止，再起動は，root のみが行えますので，一般ユーザの場合には，まず su コマンド（次項目参照）を用いて，root になってください．sync コマンドを入力した後，shutdown -h now と入力します．

```
[root@Linux00 hoge]# sync ↵
[root@Linux00 hoge]# sync ↵
[root@Linux00 hoge]# sync ↵
[root@Linux00 hoge]# shutdown -h now ↵
```

システムが停止し，電源を切ってもよいというメッセージが表示されたら，電源を切ります．最近のコンピュータを使っている場合は，シャットダウン処理の完了後，自動的に電源が切れるものもあります．

3.1.4　su　ユーザ変更

システムの設定ファイルの書き換えや，コンピュータのシャットダウンなどのシステム管理に関する作業は，root が行う必要があります．一般ユーザでログインしているときに，一時的に root になりたいときには，su コマンドを用います．

```
[hoge@Linux00 hoge]$ su ↵
Password:
```

su コマンド実行後は上記のように Password:と表示されますので，root のパスワードを入力し Enter キーを押すことで root になることができます．

3.2　ファイル操作

Linux におけるファイル操作の方法について説明します．

3.2.1　ls　ファイル名の表示

該当ディレクトリ内にあるファイルやディレクトリを表示するには，ls コマンドを用います．ただし，ls だけではディレクトリ名もファイル名も区別がつきません．ファイルの詳細が知りたい場合には，-l(エル) オプションを付けて，

```
[hoge@Linux00 hoge]$ ls -l ↵
```

と入力します．また，ls だけでは，通常は “.”（ドット） ではじまるファイルやディレクトリは表示されません．これらを表示させるには，-a オプションを付けて，

```
[hoge@Linux00 hoge]$ ls -a ↵
```

と入力します．オプションは，組み合わせて，

```
[hoge@Linux00 hoge]$ ls -al ↵
```

などとして使うこともできます.

3.2.2　mkdir, rmdir　ディレクトリ作成・消去

ディレクトリを作成するには，mkdir コマンドを用います.

```
[hoge@Linux00 hoge]$ mkdir [作成するディレクトリ名] ↵
```

と入力します．ディレクトリを削除するには，rmdir コマンドを用います.

```
[hoge@Linux00 hoge]$ rmdir [削除するディレクトリ名] ↵
```

と入力します．ただし，ディレクトリにファイルやサブディレクトリが存在する場合は削除できません．特定のディレクトリ以下をすべて削除したい場合には，後述する rm コマンドを使って

```
[hoge@Linux00 hoge]$ rm -r [削除するディレクトリ名] ↵
```

と入力します.

3.2.3　cd　カレントディレクトリの移動

自分が現在いるディレクトリのことを，カレントディレクトリといいます．カレントディレクトリを別のディレクトリに移動する時には，cd コマンドを使用します.

```
[hoge@Linux00 hoge]$ cd [移動したいディレクトリ名] ↵
```

1 つ上のディレクトリに移動したい時は “..” を用います.

```
[hoge@Linux00 hoge]$ cd .. ↵
```

ホームディレクトリに移動したい時は “ ~ ”(チルダ) を用います.

```
[hoge@Linux00 hoge]$ cd ~ ↵
```

3.2.4　cp　ファイルのコピー

ファイルのコピーをするには，cp コマンドを使います．コピー元を file1，コピー後のファイル名を file2 とすると，cp コマンドの書式は

```
[hoge@Linux00 hoge]$ cp file1 file2 ↵
```

となります．また，ディレクトリごとコピーをしたい場合には，-R オプションを付けて使います．dir1 というディレクトリを dir2 というディレクトリにコピーするには，

```
[hoge@Linux00 hoge]$ cp -R dir1 dir2 ↵
```

と入力します．

3.2.5　mv　ファイルの移動

ファイル（ディレクトリ）を移動させるには，mv コマンドを使用します．使い方は，cp とほぼ同じです．

```
[hoge@Linux00 hoge]$ mv file1 file2 ↵
```

cp コマンドと異なり，コピー元のファイルは消えてしまいますので，mv コマンドは主にファイル名やディレクトリ名を変更するために使うことが多いでしょう．

3.2.6　rm　ファイルを削除する

ファイルを削除するには，rm コマンドを使用します．file1 を削除する際には

```
[hoge@Linux00 hoge]$ rm file1 ↵
```

とします．シェルの設定によっては本当に削除していいか確認メッセージが表示される場合もあります．削除したい場合は y を，削除をやめたい場合は n を入力します．

3.2.7　less　ファイルの内容表示

ファイルの内容を表示するには，less コマンドを使用します．file1 の内容を表示する場合は

```
[hoge@Linux00 hoge]$ less file1 ↵
```

とします．ファイル表示中に使う主なコマンドは以下の通りです．

次のページを表示	Space 又は f
前のページを表示	b
次の行を表示	Enter 又は j
前の行を表示	k
ファイルの先頭に移動	g 又は <
ファイルの終端に移動	G 又は >
文字列を検索する	/[検索したい文字列]
終了する	q

3.3　エディタ

ファイル内容を書き換える編集する (= edit) ためのツールをエディタとよびます．Linux で広く使われているエディタに Emacs と vi があります．一般に，様々なアプリケーションの設定ファイルを編集する際には vi を，作業ログなどの文章を編集する際には Emacs を，という使い分けをすると良いでしょう．ここでは，これらの使用方法について説明します．

3.3.1　Emacs

Emacs の起動方法は，

```
[hoge@Linux00 hoge]$ emacs [ファイル名] ↵
```

です．

Emacs の操作は Ctrl（コントロール）キーなどを併用したキー入力で行います. たとえば Ctrl + D（Ctrl キーを押しながら D キーを叩く）が 1 文字削除です．文字の入力は，キーボードから行います．基本操作は以下の通りです．Emacs には膨大な量の操作方法があり，その全てをここで説明することは困難です．Emacs には親切にもチュートリアルガイドが同梱されていますが，操作方法をそれで覚えるのは初心者には難しいかもしれません．初心者の方は，Emacs の入門書を一冊買うのが良いでしょう．

↑ or Ctrl-P	カーソルを上に移動
↓ or Ctrl-N	カーソルを下に移動
← or Ctrl-B	カーソルを左に移動
→ or Ctrl-F	カーソルを右に移動
Ctrl + D	カーソル位置の一文字削除
Ctrl + X Ctrl + F < ファイル名 >	ファイルを開く
Ctrl + X Ctrl + S	ファイルに保存
Ctrl + X Ctrl + C	Emacs を終了

3.3.2 vi

vi の起動方法は,

```
[hoge@Linux00 hoge]$ vi [ファイル名] ↵
```

です.

vi には, テキスト入力モードとコマンドモードの 2 つのモードがあります. テキストの入力はテキスト入力モードで行い, カーソルの移動や文字の削除, コピー&ペーストなど, その他の操作はコマンドモードで行います. vi を起動した時点では, コマンドモードになっています. テキスト入力モードに切り替えるには, i キーを押します. コマンドモードに切り替えるには, Esc キーを押します. コマンドモードで行う基本操作は以下の通りです.

k	カーソルを上に移動
j	カーソルを下に移動
h	カーソルを左に移動
l	カーソルを右に移動
x	カーソル位置の一文字削除
:e [ファイル名]	ファイルを開く
:w	ファイルに保存
:q	vi を終了

vi の良いところは, シンプルでバックアップファイルを残さないところです. 設定ファイルを変更する場合には, なるべく vi を使うことを勧めます.

3.4 アプリケーションのインストール

3.4.1 rpm

最近の Linux ディストリビューションでは, 世にあまねく存在する様々なソフトウェアをパッケージ化して, インストール時に問題となる依存関係を解消しています. Red Hat Linux においては rpm と呼ばれるパッケージ管理システムが用いられています. ここでは, アプリケーションのインストールに利用される rpm コマンドについて説明します.

FTP サイトやウェブページなどから “hogehoge.rpm” といった rpm 形式のパッケージをダウンロードした場合, それをインストールする時には, i オプションをつけて rpm コマンドを実行します. rpm コマンドに i オプションをつけて実行する際には, root でなければいけません. ユーザ:hoge さんが root になり, rpm コマンドで hogehoge というパッケージをインストールする様を下に示します.

```
[hoge@Linux00 hoge]$ su ↵
Password:
[hoge@Linux00 hoge]# rpm -ivh hoghoge.rpm ↵
```

上記の例では i オプションの他に v と h オプションが並んで指定されています．v は verbose(冗長) の意味で，詳細な進捗を表示する事を意味します．また，h は進捗と一緒に #マーク (hash マーク) による進捗インジケータを表示する事を意味します．インストールする際は，i オプションだけでなく，v と h オプションをいつでも指定するようにしましょう．また，ダウンロードしたファイルを新規にインストールするのではなく，既存のパッケージをアップグレードする目的であるならば，U オプションをつけます．

```
[hoge@Linux00 hoge]# rpm -Uvh hoghoge.rpm ↵
```

インストールされているパッケージは膨大な量ですから，それらを全て覚えることはナンセンスの極みです．パッケージ名が分かっているのであれば，そのパッケージがインストールされているかどうかは，q オプションと a オプション，それから grep コマンドを組み合わせることで確認することができます．

```
[hoge@Linux00 hoge]$ rpm -qa | grep hogehoge ↵
```

q オプションは問い合わせ (query) を行い，その直後の a で全て (all) のパッケージ情報を表示するよう指定しています．そしてその後に “|” (パイプ) を介して grep コマンドで “hogehoge” を含む行のみを抽出します．その結果，hogehoge というパッケージがインストールされていれば，そのパッケージ名が表示され，インストールされていなければ，何も表示されずにコマンドプロンプトが表示されます．この問い合わせ処理は，root 権限である必要はなく，一般ユーザでも実行可能です．その他にも非常にたくさんのオプションが rpm にはあります．それらを全て説明することはここでは出来ませんので，より詳しい機能について知りたい場合は rpm のマニュアルを読むことをおすすめします．

第 4 章

ネットワークアプリケーション

4.1 FTP クライアント - gFTP

今使っているマシン A から別のあるマシン B にファイルを送りたい，あるいはマシン B にあるファイルをマシン A にダウンロードしたい，という状況があるとします．2 台のマシンの間でファイルのやりとりをするのに，フロッピーなどのメディアにファイルの書き込みをして，それをもう一方のマシンまで持っていってファイルを読み取らせる，という手段があります．しかしそのようなファイルのやりとりに 2 台のマシンで操作するのは面倒であるうえ，さらに物理的に 2 台のマシンが離れている場合，この間を移動するのが大きな問題となるでしょう．

そこで FTP が役に立ちます．FTP とは File Transfer Protocol の略で，ファイルを送信するための「約束ごと」のひとつです．FTP は，ネットワークを利用することで別のマシンとファイルの送受ができるというサービスです．使用しているマシンともう一つのマシンがどんなに離れていても，2 台のマシンがネットワークにつながってさえいれば，目の前のあなたのマシンを操作するだけでファイルの送受を行なえるのです．FTP を使用しファイルの送受を行うには，相手側のマシン (リモートホスト) が FTP サーバを稼働させていなければなりません．さらにその相手マシン (FTP サーバとなるマシン) に自分のアカウント (利用資格) がなければなりません．

また一方，インターネット上には FTP サイトと呼ばれるサイトがあります．アカウントをもたなくても誰でもファイルをダウンロードできる anonymous(匿名) FTP と呼ばれるサイトです．インターネット上の FTP サービスといえば，一般的にはこの anonymous FTP を指します．anonymous を許容するかしないかは，FTP サーバの設定によるものです．

UNIX では FTP を標準コマンドラインにより操作することができますが，Red Hat Linux には FTP をより簡単に GUI 操作できるクライアントソフト gFTP が付属されています．以下，gFTP クライアントで簡単に行えるファイルのダウンロード，アップロードの仕方について説明します．

まずはソフトを起動します．アイコンをクリックするか，シェルのコマンドラインに

gftp と入力し Enter を押してください．

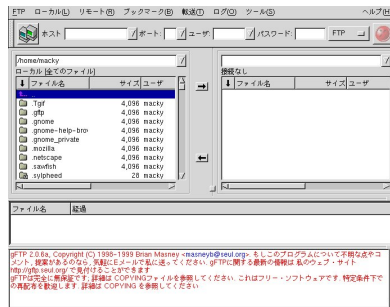



図 4.1: FTP サーバ未接続時

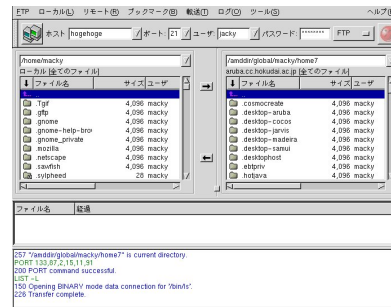



図 4.2: FTP サーバ接続時

gFTP を起動すると，画面中段の左にローカルホスト (現在のあなたの使っているマシン) の指定したディレクトリとそのディレクトリ内のすべてのファイル名が表示されています (図 4.1)．この時点ではローカルホストのファイルを参照できるだけなので，まず相手ホストを指定して接続しましょう．上の段の [ホスト] の欄に接続したい相手のホスト名，あるいは IP アドレスを入力してください．そして [ユーザ] ，[パスワード] の欄に相手ホストにあるあなたのユーザ名，パスワードを入力してください．相手ホストが anonymous を許容している場合，匿名ユーザで接続する場合は [ユーザ][パスワード] の欄に入力する必要がないことが一般ですが，必要であれば [ユーザ] の欄には「anonymous」と，[パスワード] の欄にはメールアドレスを入力してください．[ftp] あるいは [http] のプロトコルには [ftp] を選択してください．FTP にはポート番号は，20 と 21 を使っています．20 はデータ転送用，21 は制御用に使います．入力しなかったら 21 にされます．入力が終わったら Enter キーを押すか，ツールバー下のいちばん左にある，2 台のコンピュータのアイコンをクリックしてください．

すべての入力が正しいことが確認されれば接続されます．アカウントをもつユーザとして接続した場合，リモートホストのあなたのホームディレクトリが現れます．anonymous で接続したのであれば匿名ユーザ用のディレクトリが現れます．中央右にリモートホストの現在のディレクトリ，その中にあるファイル名が表示されています (図 4.2)．

まずダウンロード (ファイルの受信) の仕方です．ローカルホストでファイルを置きたいディレクトリを選択してからリモートホストのディレクトリをたどって目的のファイルを選択してください．複数のファイルをダウンロードするときは，Ctrl キーを押しながら目的のファイルを選択していきます．目的のファイルが AVI，JPEG，MPEG，プログラム, 圧縮ファイルなどバイナリ形式データならば，バイナリモードを，テキストコードからなるデータならば，アスキーモードを使います．モードの選択はツールバーの一番左の [FTP] を開き，[アスキー] か [バイナリ] のチェックを行います．ファイルを選択し，モードを選択したら中央にある左矢印のアイコンをクリックします．これでリモートホストからファイルの送信が始まり，ローカルホスト側では受信を行います．ダウンロードが終了

したら左のローカルホストの開かれているディレクトリ内に，選択されたファイルがあるのを確認してください．

アップロード (ファイルの送信) の仕方も同様で，リモートとローカルを逆に考えるだけです．リモート側のディレクトリを選択してからローカル側のファイルを選択し，右矢印のアイコンをクリックし，ファイルのアップロードが終了してからリモートホストの開かれているディレクトリの一番下にアップロードしたファイルがあるのを確認してください．

ファイルの操作が済んだら接続を解除します．ツールバーの [リモート] の中から [接続を切断] を選択してください．

4.2 Web **ブラウザ** - Mozilla

Web ブラウザ（以下，単にブラウザ）とは World Wide Web(www) で公開されている Web ページを閲覧するためのソフトウェアです．ブラウザには Netscape Navigater, Internet Explorer といった代表的なものをはじめ多くの種類がありますが，ここでは Red Hat Linux に付属の標準ブラウザ Mozilla の簡単な操作方法を説明します．

まずはソフトを起動します．アイコンをクリックするか，シェルのコマンドラインに mozilla と入力し Enter を押しましょう．

図 4.3: mozilla 画面

起動後にはホームページとして設定されているページが初めに現れます (図 4.3)．別のページに移るときはツールバーの下にあるボックスに目的の URL を入力して Enter を押してください．

日本語を標準言語としてインストールしたのなら日本語のページを読めるはずですが，日本語のページが読めなかったら，まず言語設定を行う必要があります．ツールバーの [Edit] から [Preference] を選択します．左の Category のメニューの上から 2 番目

[Navigator] を選択し，その下に現れたメニューから [Languages] を選択してください．右に新たに現れた [Languages for Web Pages] の枠内にあるボタン [Add] をクリックし，[Japanese[ja]] を選択してボックス内に Japanese[ja] が追加されたのを確認したら, [OK] をクリックしてください．一度 Mozilla を終了してから，再び起動してください．

ページ上の日本語の文字が文字化けしたらツールバーから [View] → [Character Coding] → [Auto detect] → [Japanese] と選択していってください．

4.3 up2date

セキュリティ対策の方向性はいくつかありますが，その一つとして，常にバグフィクスされた最新のアプリケーションを利用するというものがあります．アプリケーションにはほぼ必ずバグが存在し，既知のバグが修正されていないバージョンのアプリケーションを使っていると，ネットワーク経由の攻撃に対して脆弱になる可能性があります．

Red Hat Linux 8.0 ではバグが修正されアップデートされたパッケージを前述のようなFTP クライアントや WWW ブラウザを用いることで取得し，rpm コマンドで導入することもできますが，up2date という自動化的にアップデートされたパッケージを導入してインストールしてくれるシステムが用意されています．

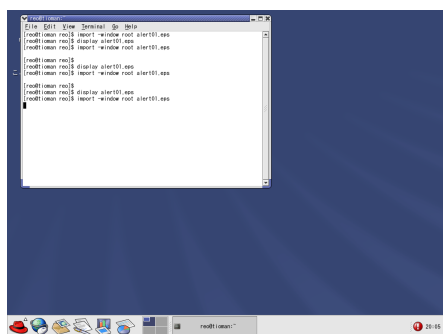



図 4.4: 初回ログイン直後の画面

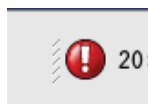



図 4.5: 赤く点灯するチェックマーク

インストール直後にログインすると，恐らく右下に赤く明滅するチェックマークが目に入ることと思われます (図 4.4, 4.5)．これが Red Hat Network 警戒通知ツールと呼ばれる仕組みで，このチェックマークをクリックすることで，自動的にアップデートが行われますが，初回は Red Hat Network に登録をする必要があります．一度登録を済ませたら，あとはログインするたびに自動的に適用可能なアップデートがないかどうかを自動的に検索し，アップデートがあれば赤色のチェックマークとなり，何もなければ青色のマークを示して教えてくれます．Windows における Windows Update の自動更新のようなものと思って頂いて差し支えないでしょう．

さて，それでは赤く明滅するチェックマークをクリックしてみましょう．初回は警戒通知ツールの初期設定画面となり，Red Hat Network への登録作業へと進むことになります

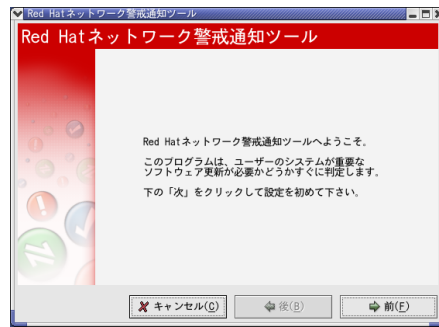



図 4.6: Red Hat Network へようこそ!

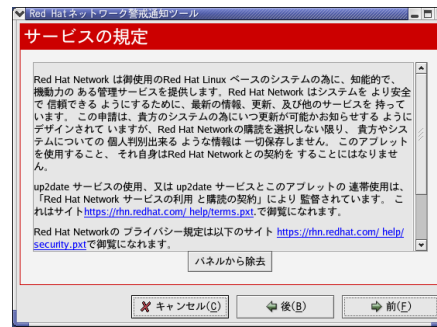



図 4.7: Red Hat Network サービス規定

まず最初に Red Hat Network への登録作業のウェルカムメッセージが表示されます (図 4.6)．ここは [前 (F)] を押して次へ進みましょう．Forward の直訳として「前」という言葉が当てられていますが,「次」じゃないのかという疑問は抱かないように心がけましょう．次にサービスの規定に関する注意事項が表示されます (図 4.7)．目を通して確認したら [前] へと進みます．

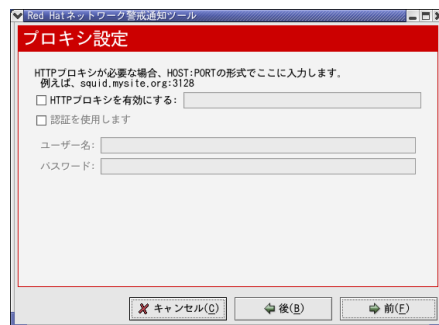



図 4.8: プロキシ設定

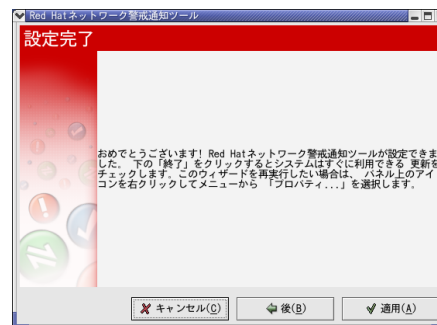



図 4.9: 設定完了

この警戒通知ツールは，新しいアップデートの確認作業を HTTP 経由で行います．そのためプロキシ設定が必要な場合は，システム管理者にその旨尋ねて設定を行う必要がありますが，北大内においてはそのような環境は稀ではないかと思われます．特に何も設定せず，設定完了後，エラーが発生するようであれば変更することにしましょう (図 4.8)．[次] を押すと，これで警戒通知ツールの設定は完了します (図 4.9)．[適用] を押して終了しましょう．

警戒通知ツールの設定が終了すると，早速アップデートを検索して利用可能なアップデートの一覧を表示してくれます (図 4.10)．ここで [up2date の起動] を押すと，ネットワーク経由でアップデートパッケージを取得してインストールしてくれるのですが，このアップデートには登録が必要です (図 4.11)．早速登録してみましょう．

up2date を実行するとパッケージが導入されるため，実行には一般ユーザではなく root 権限が必要となります (図 4.12)．root のパスワードを入れて次に進みましょう．すると次に，Red Hat Network のサーバを設定する画面となります．ここはデフォルト値で構

図 4.10: 利用可能リスト

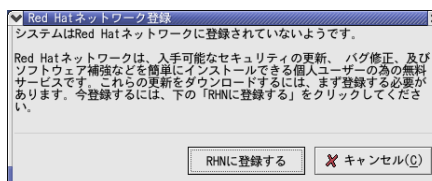



図 4.11: Red Hat Network 登録

いません．また，先ほどもあった HTTP コネクションにプロキシの設定が必要であると分かっている場合は，ここで設定しておきます (図 4.13)．

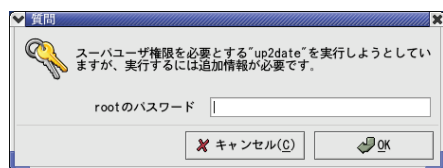



図 4.12: root パスワードの入力

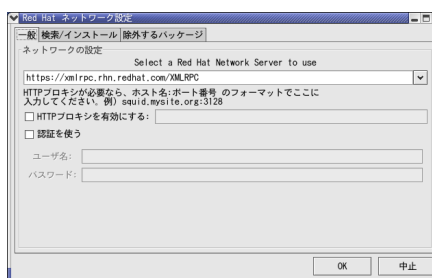



図 4.13: Red Hat Network 設定

アップデートへと入ります (図 4.14)．最初はウェルカムメッセージですので，[前] へと進みます．

実際にアップデートされたパッケージを取得するにあたり，本当にそれが Red Hat 公式のパッケージであるかを確認しないと，クラッカーにより用意されたトロイの木馬型ウィルスに感染して，まんまとセキュリティホールを作る羽目にもなりかねません．そのため，Red Hat が提供するパッケージには GPG 方式による署名が施されています．初期状態ではコンピュータにはこの Red Hat の公開鍵が存在せず，パッケージをダウンロードした時に正式なものであるかどうかの確認ができません．そのため最初に Red Hat の公開鍵をシステムに取り込む必要があります (図 4.15)．ここは素直に [はい] を選びましょう．

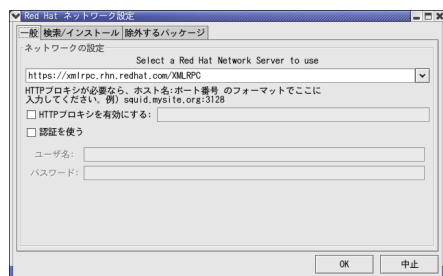



図 4.14: Red Hat Update Agent

図 4.15: GPG 公開鍵の取得

このアップデートではコンピュータの構成情報など，少なからず個人情報が Red Hat

Network 側に送信されます．そういった個人情報に関する取り扱いに関しての条項が表示されます (図 4.16)．同意できるようであれば [前] へ進みましょう．次に Red Hat Network におけるユーザアカウントを設定します．これは Red Hat Network 内で一意に定まるユーザ名を指定しなければいけないため，既に登録されているユーザ名での登録は拒否されます．既に登録されているかどうかは，実際に登録処理を行ってみるまでわかりませんので，自分が使いやすいユーザ名を入力して構いません．登録処理を行って拒否されたら変更すれば良いだけのことです．ユーザ名を入力したら，同じパスワードを上下二段に入力し，最後に E-mail アドレスを入力します．アップデートが行われるたびに，ここで入力した E-mail アドレス宛にメールが届きますので，可到達性があり，頻繁に利用するアドレスを入力しましょう (図 4.17)

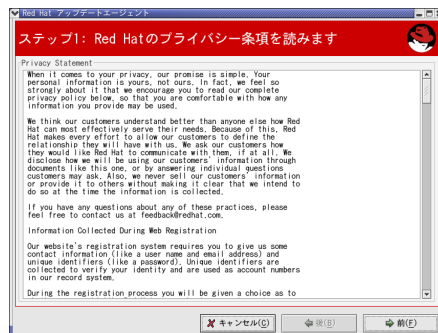



図 4.16: 個人情報について

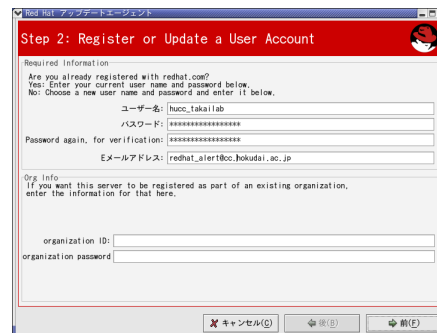



図 4.17: アカウント登録

さらにアカウント登録が続き，個人名，所属，地位，住所などを要求されますが，これらは実は空欄でも登録に支障はありません (図 4.18)．これらの情報を記入するのが面倒であったり，そこまでの個人情報を提供する必要はないと考えるならば，ここでは記入せずに次へと進んで構わないでしょう．次の項目では Red Hat Network に提出するハードウェア情報の確認が行われます (図 4.19)．ハードウェアの情報を提出することにより，適切な種類のカーネルなどをアップグレードしてくれるようになりますので，問題なければこのまま [前] へと進んでしまいましょう．

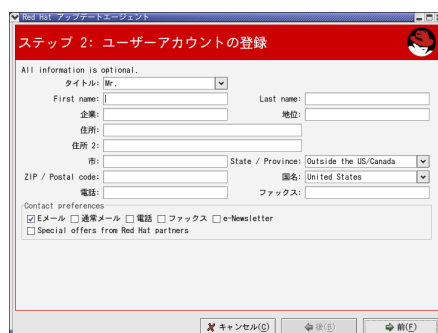



図 4.18: 続・アカウント登録

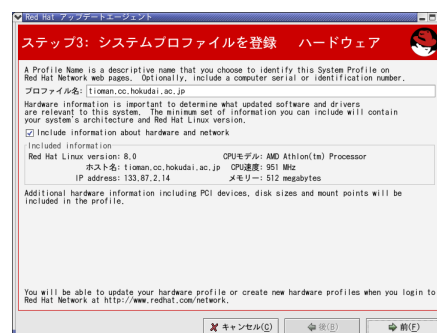



図 4.19: システムプロファイルの登録

今現在，このコンピュータのなかにどのようなパッケージが導入されているかを Red Hat Network に提出します (図 4.20)．もし，アップデートを希望しないパッケージがあれば，ここでチェックボックスを外すと，アップデートの知らせが来なくなります．特にそういった意志がなければ，ここは変更を加えないまま次へ進んで頂いて構いません．最後にこれらの情報を送信する許諾を求められます (図 4.21)．問題がなければ [前] を押して進みましょう．

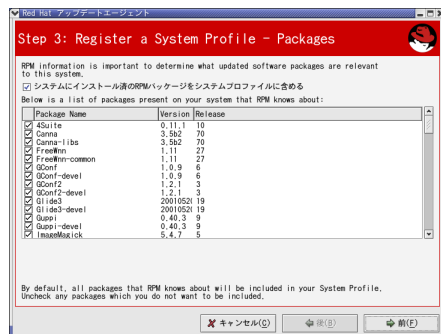



図 4.20: パッケージ登録

図 4.21: 送信確認

ハードウェア情報が送られると，Red Hat Network から適切なアップデートチャンネルが送られてきます (図 4.22)．一般的な intel x86 アーキテクチャの CPU を搭載したマシンであれば，“Red Hat Linux 8.0 i386” が表示されると思われます．それで良ければチェックボックスを ON にし (デフォルトで ON になっているでしょうから，変更する必要はありません)，[前] へと進みます．すると，次にアップデートから除外されるパッケージの一覧が表示されます．デフォルトではカーネルパッケージはアップデートしないことになっておりますが，経験的にはカーネルも自動的にアップデートして特に問題はありません．チェックボックスを ON にしてカーネルパッケージも取得する設定にしましょう (図 4.23)

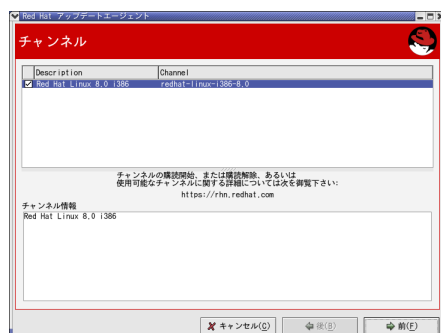



図 4.22: チャンネル登録

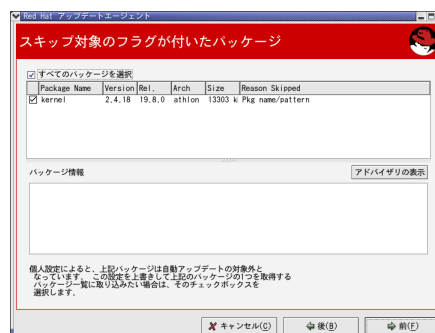



図 4.23: スキップパッケージの選択

アップデートパッケージのダウンロードが始まる前にダウンロードされるパッケージの一覧が表示されます (図 4.24)．特に除外したパッケージなどがなければ，すべてにチェッ

クがついていることを確認するだけで良いでしょう．[前] へと進むと，依存関係のチェックが行われた後，パッケージのダウンロードが始まります (図 4.25).

図 4.24: 更新パッケージの確認

図 4.25: パッケージ取り込み

パッケージのダウンロードが完了すると，インストール作業へと移行します (図 4.26). しばらく経過してインストール作業が終了すると，インストールに成功したパッケージの一覧が表示されます (図 4.27).

図 4.26: インストール中

図 4.27: 正常終了

このようにしてアップグレードパッケージがすべて導入されると，最初は赤く点灯していたチェックマークが青になります (図 4.28). この状態は，Red Hat Network 的にセキュリティが現時点で最良になっているという事を表しています．アップデートがあると，すぐに赤い点灯へと変化しますので，その場合は即座にこのチェックマークをクリックしてアップデートするように心がけましょう．

図 4.28: 正常化したチェックマーク

4.4　セキュリティレベルの設定

Red Hat Linux ではネットワークの接続制限を簡単に設定できます．インストール時にセキュリティレベルの設定という項目があるのでそのときに行うことができます．インストール後に設定を変更したい場合には次の 2 つの方法でツールを起動させて実行します．

1 つはツールバーから [GNOME メニュー (赤い帽子のマーク)] → [システム設定] → [セキュリティレベルの設定] を選択する方法で，もう 1 つは次のコマンドを入力することです．

```
[root@Linux00 hoge]# redhat-config-securitylevel ↵
```

設定ツールの実行には root 権限が必要です (図 4.29).

スーパユーザ権限を必要とする"redhat-config-securitylevel"を実行しようとしていますが、実行するには追加情報が必要です。
rootのパスワード
キャンセル(C)　OK

図 4.29: root パスワード入力画面

root パスワードを入力するとセキュリティレベルの設定画面が現れます (図 4.30).

セキュリティレベルの設定
このシステム用のセキュリティレベルを選択して下さい。
セキュリティレベル：高
デフォルトのファイヤーウォール規則を使用
カスタマイズ
信頼できるデバイス：eth0
着信を許可：WWW (HTTP) FTP SSH DHCP Mail (SMTP) Telnet
他のポート：(1029:tcp) 1234:tcp
キャンセル(C)　OK

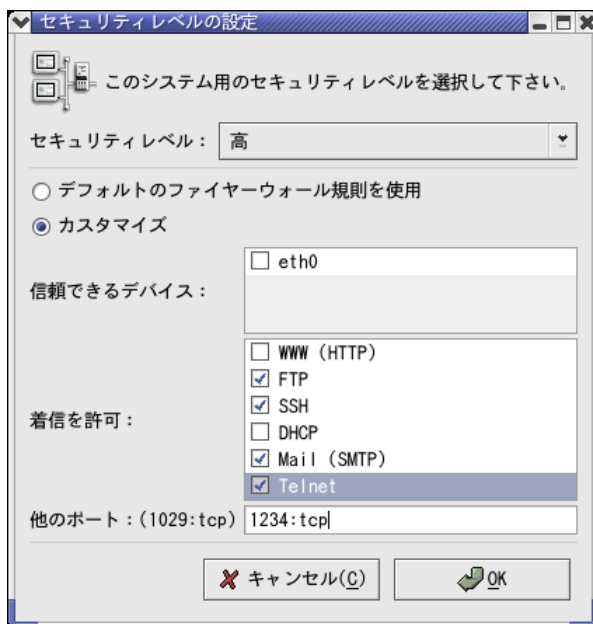



図 4.30: セキュリティレベル設定画面

ここで設定した内容は iptables のルールとしてシステムに設定されます．セキュリティレベルはデフォルトの [高]，[中]，[ファイアーウォールなし] から選択することで，それに

応じた接続制限がされます．[高] あるいは [中] を選ぶと [カスタマイズ] で許可したい接続を別途設定できます．

セキュリティレベルの設定

各レベルのデフォルトで許可される接続は次のようになっています．

- セキュリティレベル:**高**
  自ホスト以外からのアクセスを完全にシャットアウトします．
- セキュリティレベル:**中**
  特権ポート (1-1023) へのアクセスと NFS や X 関係のポートが拒絶されます．
- セキュリティレベル:**ファイアーウォールなし**
  全ての接続が許可されます．

セキュリティレベルを [高] あるいは [中] に設定のままで [デフォルトのファイアーウォール規則を使用] を選択すると他のマシンからの FTP や SSH などの接続ができなくなるので，それらの接続を許可したい場合は [カスタマイズ] で別途定義します．

カスタマイズ

ここで選んだ接続は許可されます．また， ここに無い接続を許可したい場合は，その接続が行われるポートを調べて，ポートを直接指定します．例えばポート 1234 番の TCP パケットを許可したい場合は，「1234:tcp」と追加します．また複数ポートを指定するには，それらをカンマ “,” で区切ります．ポートは次のように調べることができます．

```
[hoge@Linux00 hoge]$ less /etc/service ↵

# /etc/services:
# $Id: services,v 1.22 2001/07/19 20:13:27 notting Exp $
#
# Network services, Internet style
                                 （中略）
ftp             21/tcp
ftp             21/udp
ssh             22/tcp                          # SSH Remote Login Protocol
ssh             22/udp                          # SSH Remote Login Protocol
telnet          23/tcp
telnet          23/udp
（後略）
```

基本的には [高] にして，利用する接続を [カスタマイズ] で許可していく方法が安全です．もしも接続できないものが出てきた時，ここでの設定ミスと思われる場合は，一旦セキュリティレベルを [ファイアーウォールなし] にして確かめてみてください．これで接続できるならばセキュリティレベルを [高] に戻して [カスタマイズ] の設定を見直すことをお勧めします．

第 5 章

SSH

Linux は UNIX 系 OS であるため，コマンドラインからの操作で大概のことができるという UNIX ゆずりの長所を持っています．コマンドラインでの CUI による操作は，マウスを使うような GUI による操作に比べて圧倒的に操作に必要なデータ量が少ないため，遠隔操作に向いています．Emacs と Wanderlust などを使うとメール操作もすべて CUI で行うことができるので，学会や旅行で遠隔地へ行っても，インターネットに接続できさえすれば学内にある自分のマシンを遠隔操作していつもと変わらない操作方法でメールをチェックする事が可能です．

Linux マシンを外部から操作するための方法として TELNET を用いた遠隔操作が古くから使われて来ましたが，TELNET による操作はセキュリティ的に非常に脆弱であるためもはや全く推奨できません．そこで最近では SSH を使うのが常識となっています．SSH には SSH1 と SSH2 とがありますが，よりセキュアな SSH2 を使えるなら当然 SSH2 を使った方が良いでしょう．かつて Windows 上では SSH2 を利用するためのソフトウェアは，利用するのが難しかったり有償だったりしたため「SSH1 でも問題ないだろう」という風潮がありましたが，現在は簡単でしかも無償な SSH2 のためのソフトウェアが公開されています．もはや接続されるマシンの側（SSH サーバ）でも，SSH で接続する側のマシン（SSH クライアント）でも，SSH2 へ移行するのに何の障害も存在しません．

5.1　SSH サーバ

Linux マシンを遠隔操作するためには，その Linux マシンで SSH サーバを稼働させなければなりません．このマニュアルに記述されるようにすでにインストールされているならば，デフォルトで SSH サーバは稼働しているはずです．稼働しているかどうかの確認は，シェルプロンプトから ps コマンドを実行して行ないます．実行とその結果を以下に記します．以下で `[reo@Linux00 reo]` とあるのは Linux00 というマシン上で reo というユーザが作業をしている時のプロンプト表示です．また，↵の記号は，そこまで入力して Enter キーを押すことを意味するものとします．

```
[reo@Linux00 reo]$ ps augwx |grep sshd ↵
root     9843  0.0  0.2  2712 1244 ?      S     18:10   0:00 /usr/sbin/sshd
```

このような出力が出れば稼働しており，一行も出力がなければ稼働していないことになります．稼働していない場合，それは「SSH のパッケージが入ってはいるもののサーバが稼働していないだけ」という場合と，「パッケージ自体が入っていない」という場合とに分かれます．

パッケージが入っているかどうかの確認は rpm コマンドを使って，

```
[reo@Linux00 reo]$ rpm -qa |grep ssh ↵
openssh-3.4p1-0vl2
openssh-askpass-gnome-3.4p1-0vl2
openssh-clients-3.4p1-0vl2
openssh-askpass-3.4p1-0vl2
openssh-server-3.4p1-0vl2
```

という出力が出るかどうかで確認できます．これがない場合は，Red Hat Linux のインストール CD にも入っていますので，インストールしておきましょう．必要なものは openssh, openssh-server, openssh-clients です．クライアントは必須ではありませんが，何かと重宝することになるでしょうからインストールしておいた方が良いでしょう．

SSH サーバがインストールされていると，/etc/ssh/sshd_config という SSH サーバ設定ファイルが作成されます．この内容を vi などで変更し，SSH サーバを (再) 起動することで，設定が反映されたサービスを提供することが可能になります．

```
# $OpenBSD: sshd_config,v 1.56 2002/06/20 23:37:12 markus Exp $

# This is the sshd server system-wide configuration file.  See
# sshd_config(5) for more information.

# This sshd was compiled with PATH=/bin:/usr/bin

# The strategy used for options in the default sshd_config shipped with
# OpenSSH is to specify options with their default value where
# possible, but leave them commented.  Uncommented options change a
# default value.

#Port 22
#Protocol 2,1
#ListenAddress 0.0.0.0
#ListenAddress ::
```

sshd_config を vi などで開いてみると，最初の数行にこの設定ファイルの説明があり，次に項目とその値 (数字あるいは記号の組み合わせ) を対にする記述する行が列挙されています．行頭に#がついているのは，その行の設定を無効にするという意味ですが，設定ファイル全体を眺めてみるとほとんどすべての行頭が#であることに気づきます．これは，行頭に#がついている項目の設定値はデフォルト値であり，デフォルトの設定に変更

を加えるときは，行頭の#を消してから変更を加えます．こうすることにより，どの部分がデフォルトの設定と異なっているのかを後で見直した時に知ることが出来ます．

実際に設定を変更する時は，デフォルトの設定がなんであったのかわかるようにその行をコピーして残しておいてから変更するようにしましょう．例えば Protocol の項目を変更するとします．上記の内容を見るとわかるように，Protocol の設定はデフォルトでは

```
#Protocol 2, 1
```

と書かれています．vi で編集するならば，この Protocol の設定行にカーソルを移動させてからコマンドモードで [Y p] とすると，その行がコピー&ペーストされて

```
#Protocol 2, 1
#Protocol 2, 1
```

と一行追加されます．追加された行の行頭のコメントアウトを削除して，その行を内容を以下のように

```
#Protocol 2, 1
Protocol 2
```

と変更します．これで Protocol を 2 に設定された行が有効になります．このような手順を踏むと変更前のデフォルト値を確認しながら編集することができ，かつ変更点を元に戻す時に大変便利です．以下に示す変更すべき設定点を実際に変更するときは，上記のような手順を踏むと良いでしょう．

- Protocol
  ここで指定するのは，SSH1 と SSH2 のどちらをサポートするかです．デフォルトの “2, 1” というのは SSH2 と SSH1 の双方をサポートするという意味ですが，冒頭で述べたように「SSH2 を使用する」というのが方針なので，ここでは SSH1 のサポートを切り捨てて SSH2 のみにします．上記の例のように “2, 1” から “2” に書き換えてください．
- PasswordAuthentication
  ここで指定するのはパスワード認証を許すかどうかです．デフォルトでは “Yes” となっています．パスワード認証は，ユーザ名とパスワードを知ってさえいれば誰でも認証が出来るため，セキュリティ的に脆弱であると言えます．後ほど説明するように，今回は SSH2 の RSA 鍵を使った認証を行ないます．そのため，ここは “Yes” を “No” に書き換えます．

セキュリティの観点から見て，最低限必要な変更は上記 2 項目だけです．変更を行い，エディタ操作で sshd_config ファイルを保存してください．次に，

```
[root@Linux00 reo]# /etc/init.d/sshd restart ↵
```

として sshd を再起動させます．もともと起動していなかった場合でも，restart オプションをつけて/etc/init.d/sshd スクリプトを実行させると最終的に起動処理を行ってくれるので問題ありません．これでこのマシンは変更された sshd_config の設定を反映した SSH 接続を受け付けるようになります．

5.2　SSH クライアント

5.2.1　Windows クライアント

遠隔操作を行ってその便利さを実感するのは，自宅や出張先から研究室のマシンを遠隔操作する時でしょう．しかしながら最近では，自宅や出張先にあるマシンが UNIX 系 OS である場合の方が少ないのではないかと思われます．そこで，Windows 上で SSH2 接続を行うためのクライアントソフトウェアの導入と利用方法に関する説明を行ないます．ここでは SSH2 と RSA 鍵認証について取り上げますが，その性質上ファイルにユーザごとのアクセス制限をかけることのできる Windows NT 系 OS (WindowsNT 4.0, Windows2000, WindowsXP) での利用を推奨します．

PuTTY は Windows 系 OS 上で動作する TELNET と SSH を利用するためのオープンソースなソフトウェアです．一時配布元は

http://www.chiark.greenend.org.uk/~sgtatham/putty/

であり，今回の解説では簡便のために，このページにある「Download PuTTY!」とかかれたリンクを辿り，「A Windows-style installer (x86 only) for everything except PuTTYtel」の下にある「putty-0.53b-installer.exe」をダウンロードして話を進めることにします．

任意のフォルダに putty-0.53b-installer.exe をダウンロードして実行すると，まずインストール確認ウィンドウが表示されます (図 5.1)．

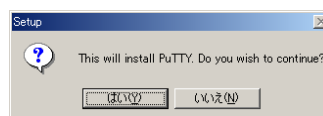



図 5.1: インストール確認ウィンドウ

[はい (Y)] ボタンを押すと，PuTTY をインストールする前に全てのアプリケーションを終了することを強く推奨する警告が出ます (図 5.2)．忠告に従って，このインストーラ以外にタスクバーにあるアプリケーションは全て終了しておいた方が良いでしょう．

[Next >] ボタンを押して次に進むと，PuTTY をインストールするフォルダを設定する画面になります (図 5.3)．デフォルトでは `C:\Program Files` フォルダ以下になりますが，Program Files フォルダに全てのアプリケーションをインストールしていくと Program Files フォルダが非常に繁雑となってしまいます．そこで Program Files フォルダの繁雑を避けるため，本マニュアルでは `C:\apps\net\PuTTY` というフォルダを作成

図 5.2: アプリケーション終了の警告

し，以下では PuTTY を `C:\apps\net\PuTTY` にインストールするものとして説明をしていきます．

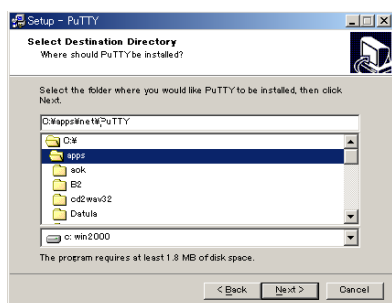



図 5.3: インストール先の設定

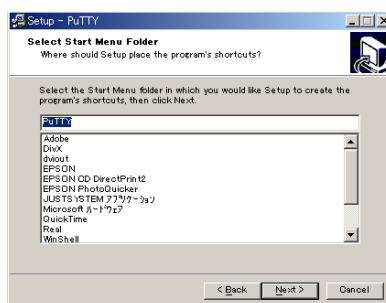



図 5.4: スタートメニューへの登録

先ほど同様に [Next >] ボタンを押して次に進むと，スタートメニューに登録する際の登録場所を尋ねられます (図 5.4)．これはデフォルトのままで問題ないので，[Next >] ボタンを押して次に進みます．

スタートメニューに登録するか，デスクトップ上にアイコンを置くか，PPK ファイルを PuTTY に関連づけするかなどを尋ねられます (図 5.5)．自分の Windows に関する知識に自信がないようであれば，これらは全てデフォルトのまま ON にしておくのが良いでしょう．

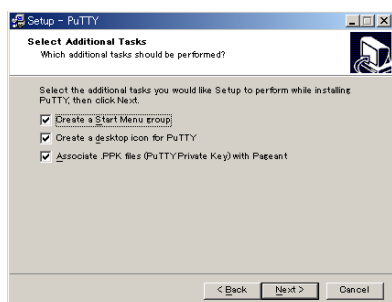



図 5.5: 各種追加設定項目

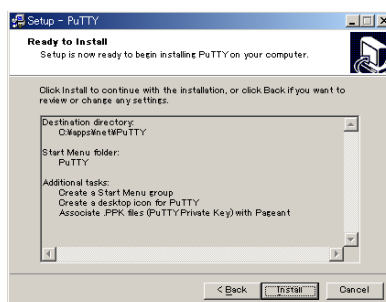



図 5.6: 最終確認

インストールの準備が整ったので，以下のようなインストール設定でよろしいですかという最終確認が表示されます (図 5.6)．特に問題なければ [Install] ボタンを押してインス

トールを開始します.

それほど大きなアプリケーションではないので，高速なマシンにおいてはインストールにかかる時間は数秒で済むでしょう．(図 5.7).

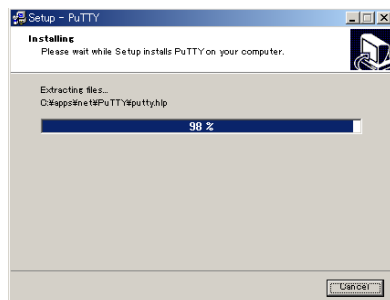



図 5.7: インストール進捗状況

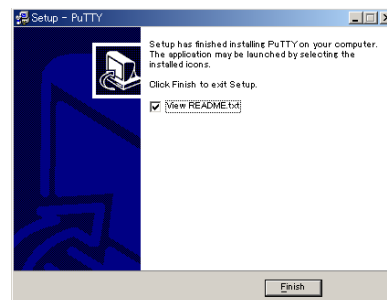



図 5.8: インストール完了

インストールが終了すると，正常にインストールが完了した旨を告げる表示が出ます．(図 5.8)．このまま [Finish] ボタンを押すと Readme.txt が表示されて，インストールは完了します.

図 5.5 の段階でデスクトップにアイコンを作成するチェックボックスを ON にしていると，デスクトップ上には PuTTY のアイコンが作成されているはずです (図 5.9).

図 5.9: PuTTY のアイコン

PuTTY は多言語化されていないソフトウェアです．そのため，例えば遠隔操作でメールのチェックをしようとしても，PuTTY では日本語の表示が化けてしまい，メールを読むことができません．そこで日本語入力と表示を実現するためのパッチをあてる必要があります.「PuTTY で ISO2022 による日本語入力・表示を可能にするパッチ」は http://hp.vector.co.jp/authors/VA024651/で公開されており，そこの「最新版ダウンロード」からリンクされているページからダウンロードする事が可能です．パッチと，すでにパッチが当てられた実行形式のファイルがダウンロード可能ですが，簡便のためにここでは実行形式のファイルを圧縮したもの (puttykjbin.zip) をダウンロードすることにします．適当なフォルダに保存し，Lhasa などの ZIP 圧縮形式を展開できるソフトウェアを使って展開し，中に含まれる puttyjp.exe と puttyjp.lng の二つのファイルを，PuTTY を保存したフォルダ (`C:\apps\net\PuTTY`) にコピーします．PuTTY をインストールした時点でデスクトップに PuTTY のアイコンが生成されているなら，そのアイコンをクリックして [プロパティ (R)] を選択し，リンク先を `C:\apps\net\PuTTY\putty.exe` から `C:\apps\net\PuTTY\puttyjp.exe` に変更すると利便性が高まります.

ここでは，SSH2 で RSA 鍵を用いた遠隔操作を実現するための方法を説明します[*1].

[*1] SSH2 では鍵認証として RSA 鍵認証と DSA 鍵認証とがありますが，DSA 鍵は署名を容易に偽造でき

SSH では経路の暗号化と鍵認証とにより，一層セキュアなシステムを実現しています．経路の暗号化は情報の盗聴を防ぎ，鍵認証は本人以外からの不正なアクセスを認証で防ぐことを目的としてます．まず，RSA 鍵認証方式で用いる公開鍵と秘密鍵を作る必要があります．インストールしたフォルダの下にある puttygen.exe を実行することによりこの鍵対を作成することができます．

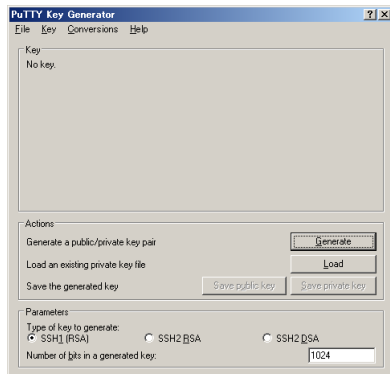



図 5.10: puttygen.exe 実行画面

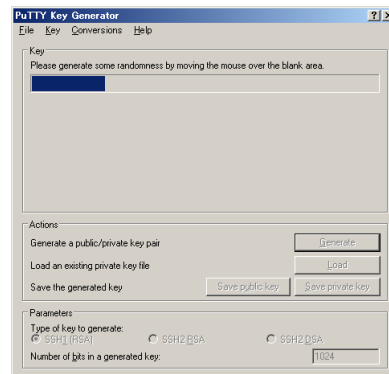



図 5.11: 鍵生成中の画面

puttygen.exe をダブルクリックして実行すると，図 5.10 に示すような画面が表示されます．画面下にある [Parameters] で囲われた項目を指定することで生成する鍵の種類を指定することができます．ここでは SSH2 RSA を指定し，鍵の強度を決定するビット数はデフォルト値の 1024 のままで構いません．これらの指定をしたら，中断にある [Generate] ボタンを押すことで鍵の生成が始まります．プログレスバーの上部に表示されるように，このウィンドウ上でマウスを適当に動かすことで生成される鍵にランダムさを与えるので，プログレスバーが右端に到着するまでひたすらマウスポインタを動かし続けなければいけません (図 5.11).

これでまず公開鍵が生成されます．次に画面に現れた [Key Passphrase] および [Confirm passphrase] の欄に，認証時に要求されるパスフレーズ（文字数の多いパスワードと考えて良いでしょう）を入力します．[Confirm passphrase] は，[Key passphrase] の欄に入力されたパスフレーズの確認用なので，同じパスフレーズを再び入力しなければいけません．双方が同一であれば秘密鍵を生成することができます．[Save public key] のボタンを押して公開鍵を保存し，[Save private key] のボタンを押して秘密鍵を保存します．ここでは後ほどの説明のため，公開鍵の名前を id_rsa.pub とし，秘密鍵の名前を id_rsa とします．

秘密鍵は自分以外の人から閲覧されてはいけません．デフォルトではこれらの鍵対は PuTTY をインストールしたフォルダに保存されます．今，PuTTY をインストールしているマシンが，自分以外誰も使わないマシンである（自分と Administrator 以外のユーザが存在しない）ならば，デフォルトで構わないません．しかし研究室で共用するマシンなどであればデフォルトのフォルダに保存することは推奨できません．自分以外にアクセス

る弱点が指摘されており，RSA 鍵の使用が推奨されています．
(→ see https://www.netsecurity.ne.jp/article/3/4470.html)

権限が設定されていないフォルダに保存してください．

これで鍵の用意はできました．次の段階として公開鍵をサーバに設置しなければいけません．最も単純かつ確実かつ推奨される公開鍵の設置方法は，公開鍵をフロッピーディスクに入れサーバマシンである Linux 側へ持って行き，鍵を読み込むという手段です．Windows 側でフロッピーをフォーマットし，公開鍵 id_rsa.pub をフロッピーディスクにコピーします．Red Hat Linux 側ではデフォルトで Gnome デスクトップ上にフロッピーディスクのアイコンがあり，ドライブにフロッピーディスクを挿入した後，フロッピーディスクのアイコンを右クリックし，[マウント] を選択すると，フロッピーディスクがマウントされて内容が表示されます．

コマンドラインからフロッピーディスクをマウントする場合は，ターミナルを開いて

```
[reo@Linux00 reo]$ mount /mnt/floppy ↵
```

によりマウントを行ないます．次にファイルマネージャーに表示された公開鍵ファイルを自分のホームディレクトリにコピーしても良いし，あるいはターミナルで

```
[reo@Linux00 reo]$ cd /mnt/floppy ↵
[reo@Linux00 reo]$ cp id_rsa.pub ~/ ↵
```

として，自分のホームディレクトリに公開鍵をコピーします．

フロッピーで公開鍵をコピーする方法以外にも，一度 Linux 側の SSH サーバの設定を，パスワード認証でログインできるように変更して，PuTTY に含まれるファイルコピーコマンド pscp を使うという手段もあります．この方法では，まず SSH サーバ側の設定ファイルで，PasswordAuthentication“Yes” として SSH サーバを再起動します．設定の変更と再起動の方法は 5.1 章を参照してください．

次に Windows でコマンドプロンプト ([スタート] → [プログラム] → [アクセサリ] → [コマンド プロンプト]) を開いて作業を行ないます．コマンドプロンプトを開くと，まず以下のように表示されます．

```
Microsoft Windows XP [Version 5.1.2600]
(C) Copyright 1985-2001 Microsoft Corp.

C:\Documents and Settings\reo>
```

最後の行の “reo” の部分はその時ログインしているユーザによって異なるので，そこは適宜読み替えてください．pscp コマンドは，PuTTY がインストールされているフォルダに存在するので，cd コマンドでそのフォルダに移動します．

```
C:\Documents and Settings\reo>cd \apps\net\PuTTY ↵
C:\apps\net\PuTTY>
```

ここで pscp コマンドを実行します．pscp コマンドの書式は

```
pscp [コピーしたいファイル名] [サーバでのユーザ名]@[サーバ名]:[コピーする場所]
```

です．id_rsa.pub を，“Linux00” という名前のサーバにある “reo” というユーザのホームディレクトリにコピーしたい場合は

```
pscp id_rsa.pub reo@Linux00:~/
```

となります．最後の “~/” はホームディレクトリを表します．上記のコマンドを実行すると以下のようになります．

```
C:\apps\net\PuTTY>pscp id_rsa.pub reo@Linux00:~/ ↵


The server's host key is not cached in the registry. You
have no guarantee that the server is the computer you
think it is.
The server's key fingerprint is:
1024 fe:88:b9:f8:30:01:9f:c3:e5:c4:35:14:12:33:ae:d2
If you trust this host, enter "y" to add the key to
PuTTY's cache and carry on connecting.
If you want to carry on connecting just once, without
adding the key to the cache, enter "n".
If you do not trust this host, press Return to abandon the
connection.
Store key in cache? (y/n)
```

初めて pscp を利用した時は，このように情報をキャッシュするかどうかの確認が求められます．y を選択すれば接続ホストの情報がキャッシュされ，n を押すとキャッシュされません．Enter キーのみ押すと接続をしないで終了します．ここは y を選択してください．

```
Store key in cache? (y/n) y↵
reo@Linux00's password:
```

y を選択すると，Linux00 に reo としてアクセスする際のパスワードを訪ねられるので，入力して Enter キーを押します．この際，画面には自分の入力したパスワードはもとより，*印なども全く表示されません．パスワードが正しければ，ファイルのコピーが始まります．

```
reo@Linux00's password:                ↵
id_rsa.pub             |          0 kB |   0.3 kB/s | ETA: 00:00:00 | 100%
C:\apps\net\PuTTY>
```

これで，サーバのホームディレクトリに公開鍵をコピーすることができました．

フロッピーで持っていっても，pscp を使っても，SSH サーバ側に puttygen.exe で生成した公開鍵をコピーできたら，今度は鍵の内容を所定のファイルに登録しなければなりません．フロッピーで鍵を持っていったのであれば SSH サーバ上で直接操作することが可能です．pscp を使ったのであれば，puttyjp.exe を実行し，最初の画面でホスト名の部分に SSH サーバ名を，その下にあるプロトコルで SSH を選択してウィンドウ下部の [開く(O)] ボタンを押せばパスワード認証で SSH サーバに入ることができます．

ホームディレクトリに置いてある id_rsa.pub は，SSH サーバである OpenSSH の規格とは異なるフォーマットの鍵形式のため，これを変換して所定のファイルに追加する必要があります．この作業のためには，以下のように ssh-keygen コマンドを実行します．

```
[reo@Linux00 reo]$ ssh-keygen -i -f id_rsa.pub >> ~/.ssh/authorized_keys ↵
```

ssh-keygen のオプション -i は，OpenSSH 互換の公開鍵を出力するためのオプションであり，その後の -f オプションで，変換される公開鍵を指定しています．~/.ssh/authorized_keys というのが認証の確認の際に用いられる所定のファイルです．このファイルに様々な公開鍵を追加していくことにより，様々なクライアントから接続できるようになります．これで SSH サーバ上の操作は終了です．pscp や puttyjp を使って作業した場合は，SSH サーバの設定を元に戻してパスワード認証が出来ないようにしておきましょう．

あとは puttyjp.exe を実行して，適切に設定するだけで接続することができます．デスクトップ上にある PuTTY のアイコンか，あるいはインストールしたフォルダにある puttyjp.exe を実行します．初期状態では以下のような画面になるはずです (図 5.12).

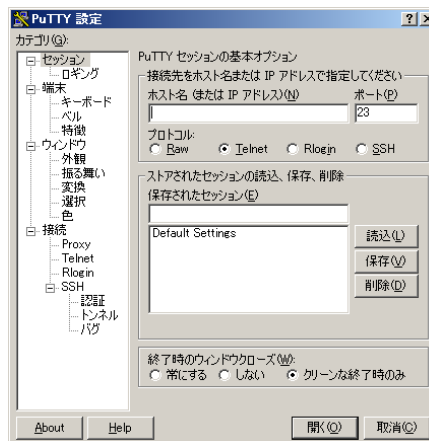



図 5.12: puttyjp.exe 実行画面

画面の左側に各設定カテゴリが表示され，右側に設定項目が表示されるインターフェイスで設定します．以下，各設定カテゴリごとに説明を進めていきます．最初の「セッション」のカテゴリでは，最も基本的な設定を行ないます．「ホスト名 (または IP アドレス)」と書かれた項目に，SSH サーバの名前 (例えば Linux00.cc.hokudai.ac.jp などのように)

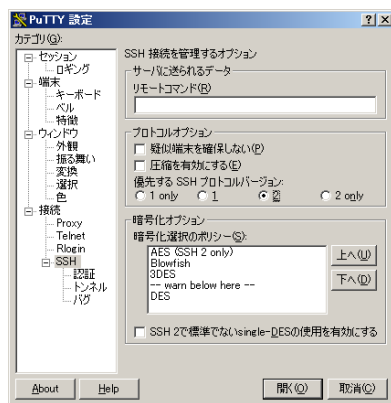



図 5.13: SSH カテゴリ設定画面

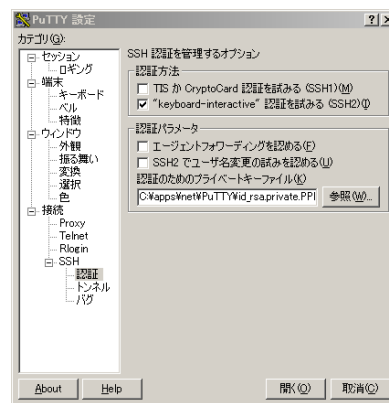



図 5.14: SSH 認証カテゴリ設定画面

を入力し，その下の「プロトコル」では SSH を選択します．「ポート」は SSH を選択した時点で自動的に変更されるので入力する必要はありません．その下にある「ストアされたセッションの読込，保存，削除」という欄では，設定全体をセーブすることができ，セーブされた設定を読み込んで即座に接続することが可能です．設定が全部終わってからセーブすることにします．

次に重要な設定は「接続」カテゴリの下にある「SSH」です．このカテゴリにある「優先する SSH プロトコルバージョン」を「2」あるいは「2 only」にしておきましょう (図 5.13)．次に「SSH」カテゴリの下層にある「認証」カテゴリで,「認証のためのプライベートキーファイル」の設定を行います．入力フィールドの右側にある [参照] ボタンを押し，保存した秘密鍵を指定します (図 5.14)．

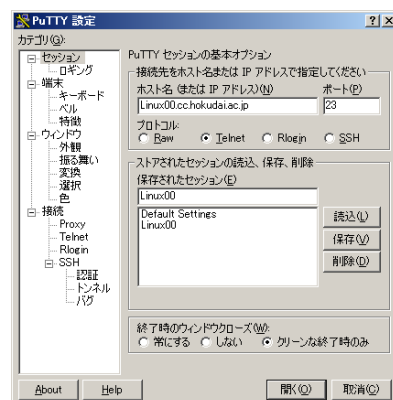



図 5.15: セッション登録画面

これらが接続に必要な最低限の情報ですが，この他にウィンドウの大きさや色，フォントなどを個人的嗜好にあわせて変化させても良いでしょう．最後に「セッション」カテゴリに戻り，設定した項目をセッションとして保存します．「保存されたセッション」のフィールドに任意の名前（例えば接続するホスト名からとって Linux00 といったように) を入力して，[保存] ボタンを押します．するとボタンの左側にあるリストにセッションが新規追加されるので，今後 PuTTY を起動したら，このセッション名をダブルクリックすることで接続することができるようになります (図 5.15)．

今，設定したセッション情報で接続するためにはウィンドウ右下にある [開く] ボタンを押します．するとウィンドウが開いて，

```
login as:
```

と表示されるので，ログインするユーザ名を入力して Enter キーを押します．次に

```
Authenticating with public key "rsa-key-20021220"
Passphrase for key "rsa-key-20021220":
```

のような表示があるので，表示の後に続いて，秘密鍵を作った際に入力したパスフレーズを入力して Enter キーを押します．パスフレーズが正しければ，以下に示すような画面が表示され，接続が成功します．接続に成功したら自由に遠隔操作できます (図 5.16)．

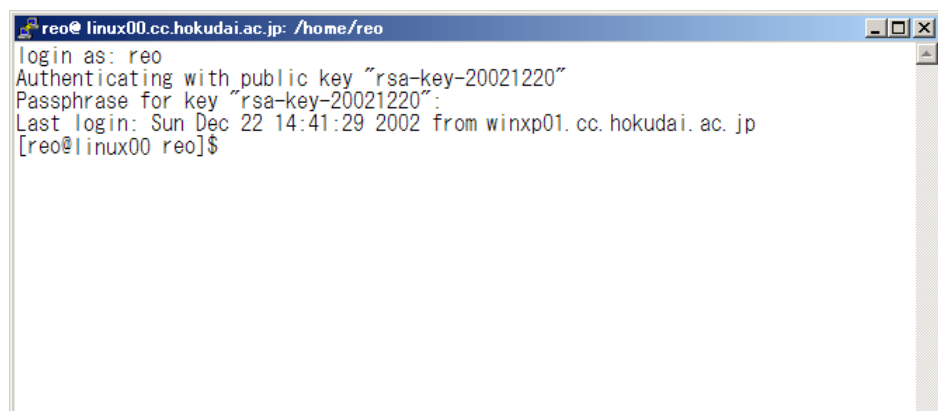



図 5.16: 接続成功時の画面

5.2.2　Linux クライアント

研究室という環境では複数の Linux マシンがあることが想定されます．ある一つの Linux マシンから別の Linux マシンを操作できたら，効率がはかどり快適に作業をすることができるでしょう．

そのような想定から，この章では Linux 上で SSH2 接続を行うためのクライアントソフトウェアの導入と利用方法に関する説明を行ないます．ここで，SSH サーバである Linux マシンの名前を Linux00 とし，クライアントとなる Linux マシンを Linux01 として説明をすすめます．

Linux 用の SSH クライアントは openssh-client というパッケージで提供されます．このパッケージはデフォルトで入っているはずですが，5.1 章で説明したように，rpm コマンドで確認して入っていないようであれば Red Hat Linux のインストール CD や up2date システムなどを利用してインストールします．

Windows での PuTTY と同様に，Linux での openssh-client でも，最初に鍵対を生成する必要があります．openssh-client に含まれている鍵生成プログラムは ssh-keygen で

す．ssh-keygen の書式は

```
ssh-keygen -t [鍵の種類]
```

という -t オプションのみを覚えておけば良いでしょう．ここで鍵の種類として “rsa” を指定すると，SSH2 用の RSA 鍵が生成されます．

```
[reo@Linux01 .ssh]$ ssh-keygen -t rsa ↵
Generating public/private rsa key pair.
Enter file in which to save the key (/home/reo/.ssh/id_rsa):
```

鍵の保存場所とファイル名を尋ねられますが，デフォルトの保存場所と名前 (/home/reo/.ssh/id_rsa) が同時に提示されます．デフォルトで問題ないので，ここでは Enter キーを押します．

```
Enter file in which to save the key (/home/reo/.ssh/id_rsa): ↵
Enter passphrase (empty for no passphrase):
```

次にパスフレーズを尋ねられます．5.2.1 章でも述べたように，パスフレーズとは文字数の多いパスワードのようなものです．キーボードの入力に対してパスフレーズ本体は当然として＊マークも表示されないことに注意してください．入力し終わったら Enter キーを押し，もう一度確認のためのパスフレーズを入力して再度 Enter キーを押します．

```
Enter passphrase (empty for no passphrase):                    ↵
Enter same passphrase again:                ↵
Your identification has been saved in /home/reo/.ssh/id_rsa.
Your public key has been saved in /home/reo/.ssh/id_rsa.pub.
The key fingerprint is:
6b:d0:6a:ed:52:9c:45:e6:cc:9b:8c:c7:a0:c3:1a:16 reo@Linux01.cc.hokudai.ac.jp
```

すると~/.ssh 以下に公開鍵 id_rsa.pub と秘密鍵 id_rsa が生成されます．この公開鍵を SSH サーバに持っていく方法は Windows と同じで，フロッピーディスクに入れて持って行くか，あるいは一度サーバの設定を変更して scp を使うかです．Linux でフロッピーディスクを初期化するには，デスクトップ上にあるフロッピーディスクのアイコン上で右クリックをして [Format floppy] を行えば良いのですが，シェルプロンプト上でフォーマットをする方法も解説しておきます．

1.44MB のフロッピーディスクをディスクドライブに入れて以下のように fdformat コマンドを実行します．

```
[reo@Linux01 .ssh]$ fdformat /dev/fd0H1440 ↵
両面，80 トラック，18 セクタ/トラック．合計容量 1440 kB．
フォーマットします ... 終了
照合します ... 終了
[reo@Linux01 .ssh]$
```

これはフロッピーディスクの物理フォーマットなので，次にフロッピーディスクにファイルシステムを作成する必要があります．mkfs コマンドを以下のように実行します．

```
[reo@Linux01 .ssh]$ /sbin/mkfs -t ext2 /dev/fd0H1440 ↵

mke2fs 1.29 (24-Sep-2002)
Filesystem label=
OS type: Linux
Block size=1024 (log=0)
Fragment size=1024 (log=0)
184 inodes, 1440 blocks
72 blocks (5.00%) reserved for the super user
First data block=1
1 block group
8192 blocks per group, 8192 fragments per group
184 inodes per group

Writing inode tables: done
Writing superblocks and filesystem accounting information: done

This filesystem will be automatically checked every 25 mounts or
180 days, whichever comes first.  Use tune2fs -c or -i to override.
[reo@Linux01 .ssh]$
```

これでフォーマットは完了です．Linux で広く使用されているファイルシステムである ext2 でフォーマットしているので，デフォルトでは MS-DOS 形式でフォーマットされたディスクをマウントできないディストリビューション (例えば Debian) などに持って行ったとしても問題なく読み込む事ができます．

それでは公開鍵をフロッピーディスクにコピーします．

```
[reo@Linux01 .ssh]$ mount /mnt/floppy ↵
[reo@Linux01 .ssh]$ cd /mnt/floppy/ ↵
[reo@Linux01 floppy]$ cp ~/.ssh/id_rsa.pub ./ ↵
[reo@Linux01 floppy]$ cd ~ ↵
[reo@Linux01 reo]$ umount /mnt/floppy ↵
```

上記では最初にフロッピーディスクをマウントする操作を行います．次にフロッピーディスクに移動して，公開鍵をコピーし，ホームディレクトリに戻り，フロッピーディスクを

アンマウントするという作業を行ってます.

次いでフロッピーディスクを SSH サーバ側に持っていき，コピーをして所定のファイルに公開鍵を追加します.

```
[reo@Linux00 reo]$ mount /mnt/floppy ↵
[reo@Linux00 reo]$ cp /mnt/floppy/id_rsa.pub ~/.ssh ↵
[reo@Linux00 reo]$ cd ~/.ssh ↵
[reo@Linux00 reo]$ cat id_rsa.pub >> authorized\_keys
```

これで SSH サーバ側での作業は終了です．SSH クライアント側から ssh コマンドを実行すれば接続することができます.

```
[reo@Linux01 ~]$ ssh Linux00 ↵
Enter passphrase for key '/home/reo/.ssh/id_rsa':
```

と，パスフレーズの入力を求められます．ssh-keygen で鍵対を作成した時に設定したパスフレーズを入力して Enter キーを押します.

```
Enter passphrase for key '/home/reo/.ssh/id_rsa':          ↵
```

パスフレーズが正しければ，ログインに成功するはずです.

SSH での接続は TELNET と比べれば，その準備は繁雑と言えます．しかし，通信路の暗号化により盗聴や傍受によるパスワード等個人情報の漏洩を防ぐことが出来ます.「研究室内に限っては TELNET で問題ない．むしろ SSH を導入することは性悪説に基づくものだ」という意見も聞かれますが，どんなネットワーク管理者であれ，不審者が研究室に侵入していくつかのネットワーク機器をとりかえて盗聴を行う準備を整えることまで検知することは困難です．管理者に万能を求めるよりも，ユーザー一人一人が SSH などを使って盗聴や傍受の対策を行ってセキュアなシステムを構築することの方が現実的と言えるでしょう.

第 6 章

Webmin

6.1 Webmin とは

Webmin は Linux の様々な設定を GUI を使って行うことができるツールです．その設定は非常に充実していて，システムの基本設定からインターネットサーバの設定など幅広く対応しています．また，Web ブラウザがフロントエンドであるため，Windows や MacOS などが動作している他の PC からも操作ができます．ただし，その際はセキュリティに十分注意する必要があります．

6.2 Webmin のインストール

まず，Webmin をインストールする必要があります．

6.2.1 インストールの確認

Webmin がインストールされているかどうかは次のコマンドで調べます．

```
[hoge@Linux00 hoge]$ rpm -aq | grep webmin ↵
```

インストールされていれば

```
[hoge@Linux00 hoge]$ rpm -aq | grep webmin ↵
[hoge@Linux00 hoge]webmin-1.070-1
```

このようなバージョンが表示されます．表示されなかった場合は，次に説明する方法でインストールを行ないます．

6.2.2 インストール

先ず，Webmin の公式ページ http://www.webmin.com/webmin/ へ行き，最新版の RPM ファイルをダウンロードします．そして，root になり

```
[root@Linux00 hoge]# rpm -ivh webmin-1.070-1.noarch.rpm ↵
```

としてインストールを実行します．(2003 年 2 月 20 日現在では Webmin の最新のバージョンは webmin-1.070 です．)

```
[root@Linux00 hoge]$ rpm -ivh webmin-1.070-1.noarch.rpm ↵

Operating system is Redhat Linux 7.2\\
webmin  ###########################################################
Webmin install complete.
You can now login to https://linux00.cc.hokudai.ac.jp:10000/
as root with your root password.
```

無事インストールが終わったら Webmin を実行することができます．

6.2.3　実行

Webmin はブラウザで実行されるので，まず Mozilla などのブラウジングツールを実行します．そして，アドレスとして次のいずれかを入れることで Webmin が実行されます．

・https://localhost:10000/　　ローカルからアクセスする場合
・https://Linux00:10000/　　ホスト名を入力する場合 (例：ホスト名が Linux00 のとき)
・https://vvv..xxx.yyy.zzz:10000/　　マシンの IP アドレスを入力する場合

インストールが成功していれば，Webmin のログイン画面が表示されるます (図 6.1)．［Username］欄に「root」，［Password］欄に root のパスワードを入力して［ログイン］ボタンをクリックします．すると，Webmin の画面が表示されます (図 6.2)．

図 6.1: ログイン画面

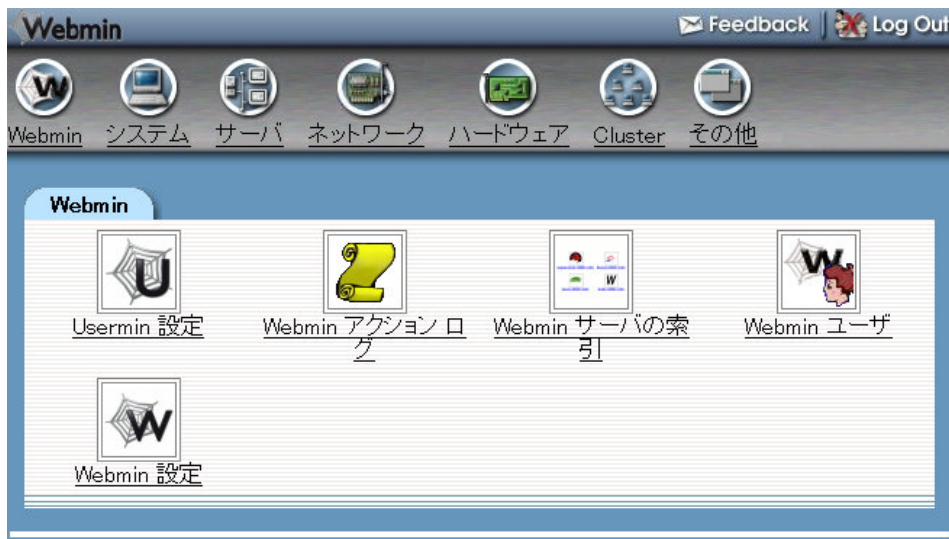



図 6.2: Webmin インデックス画面

6.2.4　日本語化

日本語表示は Red Hat Linux にはインストールされないので，自分でインストールする必要があります．［Webmin Configuration］アイコンをクリックすると，Webmin 設定の画面に移ります (図 6.3)．この画面から［Language］アイコンをクリックします．言語の選択ボックスが表示されるので，［Japanese（JA_JP.EUC)］を選択して［Change Language］ボタンをクリックします (図 6.4)．以上の操作で，表示が日本語になります．

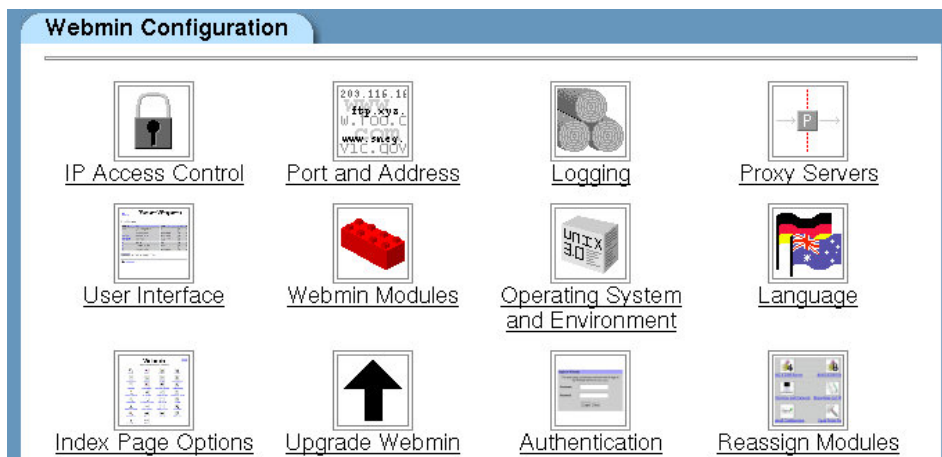



図 6.3: Webmin 設定インデックス画面

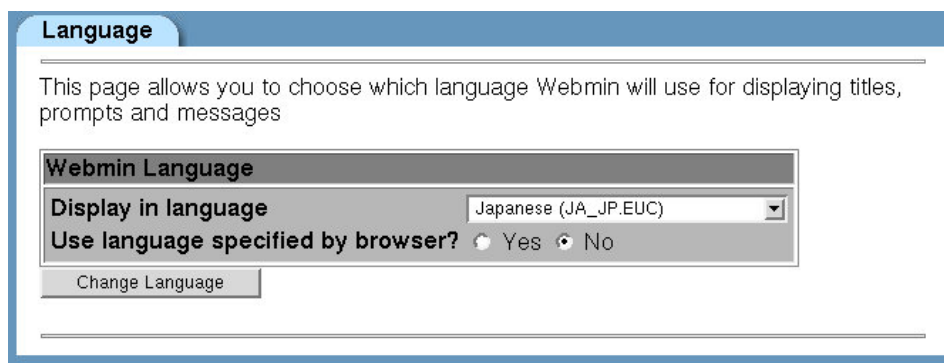



図 6.4: 日本語化画面

6.3 SSL 暗号化

6.3.1 OpenSSL

Webmin は，Web ブラウザでシステム設定が行える便利なツールですが，反面パスワードがネットワーク上を流れ，第三者から盗聴される危険性があります．SSL はそのような危険を防ぐためのもので，Web ブラウザとサーバー間の通信を暗号化し，より安全にネットワーク通信を可能にするものです．

まず，OpenSSL がインストールされている必要がありますが，多くの Linux ディストリビューションではインストール済みかも知れません．下記のコマンドで確認してみて下さい．

```
[hoge@Linux00 hoge]\$ rpm -qa | grep openssl ↵
```

これで表示されなかった場合は，CD-ROM や FTP サイトから次のようにインストールしてください．

```
[root@Linux00 hoge]# rpm -ivh openssl-xx.yy.rpm ↵
```

6.3.2 Net::SSLeay

次に， Webmin で OpenSSL を利用するために Net::SSLeay をインストールします．Net::SSLeay.pm のホームページ http://www.bacus.pt/Net_SSLeay/ からダウンロードしてください．ただし，インストールに際しては予め OpenSSL がインストールされている場合，そのバージョンに合ったものをインストールしなければうまくいきませんので注意してください．

インストール方法 1

ダウンロードしたファイルを自分で解凍してインストールします．

```
[hoge@Linux00 hoge]$ gunzip -c Net\_SSLeay.pm-1.07.tar.gz | tar xvf - ↵
[hoge@Linux00 hoge]$ cd Net\_SSLeay.pm-1.07/ ↵
[hoge@Linux00 hoge]$ ./Makfile.PL -t ↵
[hoge@Linux00 hoge]$ su ↵
[root@Linux00 hoge]# make install ↵
```

インストール方法 2

Webmin を起動して [その他] → [Perl モジュール] と進み [ローカルファイルから] で [Net_SSLeay.pm-1.07.tar.gz] を選んで [インストール] をクリックします．
すると，［Perl モジュールのインストールオプション］というオプション選択の画面が表示されます．［インストールアクション］を［make してインストール］にして，［Makefile.PL 引数］の欄に「/usr」と入力したら［インストールを続行］ボタンをクリックします．すると，モジュールの展開やコンパイルなどが始まります．

6.3.3 SSL 有効化

Webmin より先に OpenSSL をインストールしてある場合は，インストールの途中に SSL 暗号化を有効にするかを聞かれるので有効にします．Webmin 導入済だった場合は，Webmin を起動して [Webmin] → [Webmin 設定] → [SSL 暗号化] と選択して進み，[SSL サポート] の欄の [Enable SSL if available?] を [はい] にして保存すれば，有効になります (図 6.5)．今後，Web ブラウザの「セキュリティの警告」ダイアログボックスが表示されますが，そのまま続行します．以降のアクセスは，自動的に暗号化されます．

6.4 各種設定

インデックス画面の各設定のアイコンを見ると，Webmin では様々な設定ができることがわかります．しかし，全てが使い易いと言うわけではなく，直接ファイルを編集して設定を行う方が簡単で融通の効くこともあります．
そこで，Webmin を使うと良いと思われる項目についてカテゴリ別にわけて説明していきます．

6.4.1 Webmin

Webmin 画面上にある [Webmin] アイコンをクリックしてください．Webmin インデックス画面に移ります (図 6.4)．

Webmin の設定

SSL サポート
Enable SSL if available? はい いいえ
Private key file /etc/webmin/miniserv.pem
Certificate file Same file as private key
保存

This form can be used to create a new SSL key for your Webmin server.

Create SSL key
Server name in URL Any hostname localhost
E メール アドレス root@hoge.cc.hogeuniv.ac.jp
部門
組織 Webmin Webserver
州
国コード
Write key to file /etc/webmin/miniserv.pem
Use new key immediately? はい いいえ
Create Now

図 6.5: SSL 有効化

■IP アドレスの制御　他のマシンからの Webmin の実行を IP アドレスで制限できます．制限する際は，現在アクセスしているマシンの IP アドレス (ローカルなら 127.0.0.1) を許可しないとエラーになるので注意してください．

■プロキシサーバー　HTTP や FTP での接続の際に使用するプロキシサーバーを設定できます．

■Webmin のアップグレード　最新版の Webmin にアップグレードすることができます．

■SSL 暗号化　先に述べたように SSL 暗号化を有効にするかを設定できます．

6.4.2 システム

Webmin 画面上にある [システム] アイコンをクリックして下さい．システムインデックス画面に移ります (図 6.6)．

■Change Passwords　既に存在するユーザのパスワードを変更します．一覧からパスワードを変更したいユーザー名を選択してください．パスワード変更の画面が表示されます．新しいパスワードを入力し，[Change] を押してください．

■Filesystem Backup　Linux では，dump，restore コマンドを使用して，ファイルシステムのバックアップを行います．dump コマンドは，ファイルシステムのバックアップを，restore コマンドは，ファイルの復元を行います．Webmin では，簡単な操作でこの作業を行うことができます．dump コマンドがインストールされていない場合は，CD-ROM

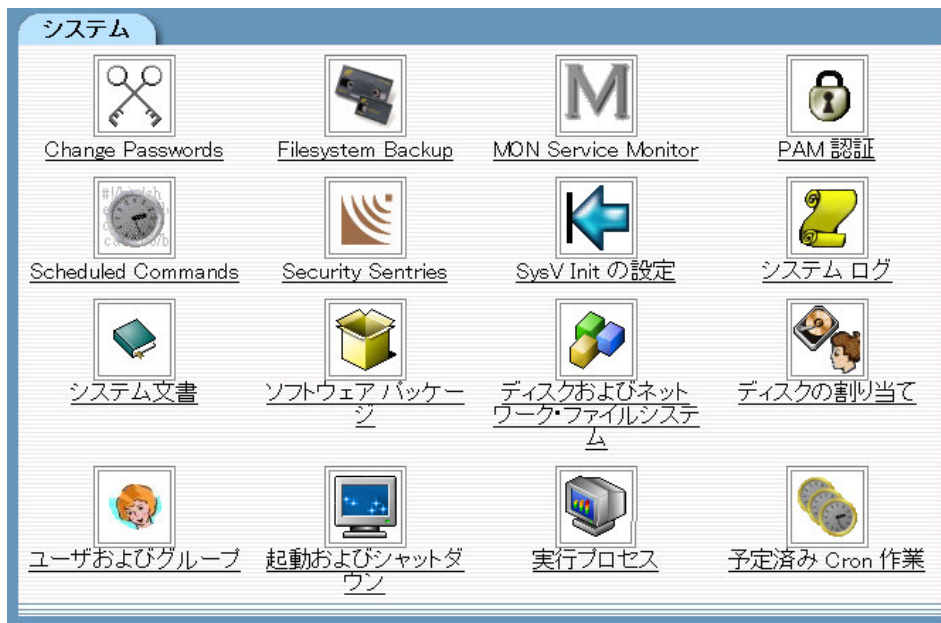



図 6.6: システム インデックス画面

や FTP サイトから次のようにインストールしてください．

```
[root@Linux00 hoge]# rpm -ivh dump-0.4b28-4.i386.rpm ↵
```

dump の設定を行うには，バックアップするファイルシステムのマウントポイントを入力し，[Add a new backup of directory:] を押します．

各設定項目の内容は以下の通りです．

Directory to backup	入力したバックアップするファイルシステムのマウントポイントが表示されます.
Backup to	バックアップするファイル名，テープデバイスなどを入力します.
Update /etc/dumpdates file?	「はい」をチェックすると，インクリメンタルバックアップ（差分のみバックアップ）に備えて，/etc/dumpdates を更新します./etc/dumpdates は，インクリメンタルバックアップのときに参照されます.
Split across multiple files?	1 つのファイルの最大サイズの制限が小さいファイルシステムにバックアップする場合，このオプションを指定することにより，バックアップファイルを分割して保存することができます.
Dump level	dump のレベルを設定します．level には，ファイルシステム全体をバックアップするレベル 0 と，インクリメンタルバックアップの，レベル 1〜9 までがあります.
Backup label	後でこのバックアップを見分けるために使用できます.
Scheduled backup enabled?	Enable にすると，画面下部の時間設定を行うことにより，dump の自動バックアップの設定が行えます．すぐにバックアップを実行したい場合は,「Create and Backup Now」をクリックします.
Email scheduled output to	自動バックアップを設定した場合，ここに入力した E-mail アドレスに実行結果が送信されます.

リストアするには，最初の画面のプルダウンリストからファイルシステムのタイプを選択し，[Restore backup of filesystemtype:] を選択します．各設定項目の内容は以下の通りです.

Restore from file or device	dump でバックアップされたファイル，またはテープデバイスから，restore するものを指定します.
File to restore	[Listed files...] を選択すると，指定したファイルだけを取り出すことができます.
Restore to directory	restore するディレクトリを指定します.
Backup is split across multiple files	バックアップのときに「Split across multiple files?」を有効にした場合は，これを選択します.
Only show files in buckup?	「はい」を選択すると，実際にはリストアを行わずに，リストアされるファイルのリストを表示します.

■ディスクおよびネットワークファイルシステム CD-ROM やフロッピー，ネットファイルシステムのマウントをすることができます.

■ユーザおよびグループ　新規ユーザやグループを追加できます．ユーザを追加するには [新しいユーザの作成] をクリックし，作成手順にしたがってアカウントを追加していきます．なお，パスワードは [通常のパスワード] を選択してユーザパスワードを入力してください．

■実行プロセス　現在の実行プロセスが確認できます．

[ユーザ] をクリックするとプロセスがユーザ別に分類されます．また，プロセスの CPU，メモリの占有率も見ることができます．[検索] をクリックすると，様々な条件で実行されているプロセスが検索できます．

6.4.3　サーバ

Webmin 画面上にある [サーバ] のアイコンをクリックして下さい．サーバインデックス画面が現れ (図 6.7)，各種サーバの設定を行なうことができますが，ここではその中の SSH サーバと WU-FTP サーバの設定を説明します．

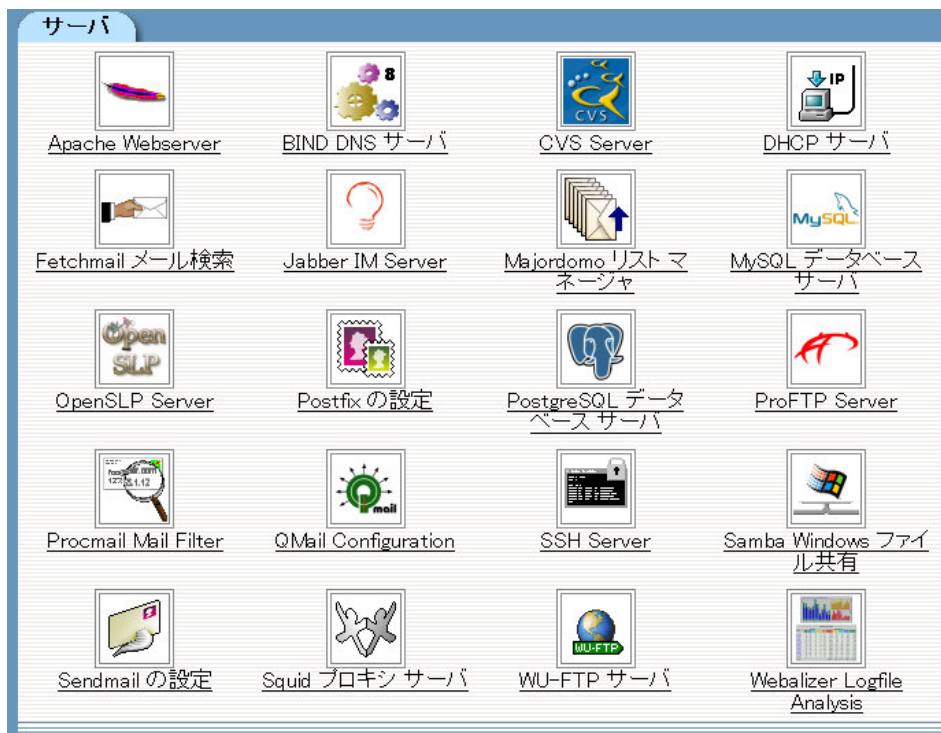



図 6.7: サーバ インデックス画面

SSH サーバ

SSH について詳しいことは第 5 章を読んで下さい．第 5 章では設定ファイル `/etc/ssh/sshd_config` を直接編集することで SSH サーバの設定をしました．ここでは Webmin を使っての SSH サーバの設定を説明します．5 章を踏まえた上での説明なの

で，openssh-server がインストールされていることとします．インストールされていなければ第5章を参照してインストールしてください．

まず Webmin サーバ画面から [SSH Server] のアイコンをクリックして下さい．SSH Server の画面が現れます (図 6.8)．この画面からの操作で SSH サーバを設定します．以下，最低限の重要な設定操作を説明します．

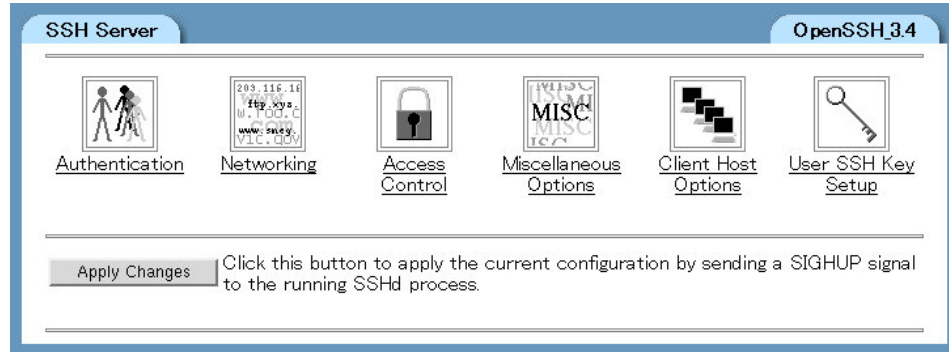



図 6.8: SSH Server モジュールインデックス画面

■Authentication　(**認証の設定**)　ここではセキュリティ上でパスワード認証よりも安全な **RSA 認証を使用する**ことにします．RSA とは公開鍵暗号方式の一つであり，その鍵の解読は極めて困難なため，盗聴の危険性を低くすることができるものです．

[Allow RSA authentication?] のチェック欄を確認してください．デフォルト (起動直後設定を変更していない状態) では [はい] となっていますが，もし [いいえ] になっていれば [はい] にチェックをいれて下さい．そして [Allow authentication by password] のチェックを [いいえ] にします (図 6.9)．

図 6.9: Authentication の設定

設定を変更したら [保存] をクリックしてください．

■Networking　(**接続の設定**)　前章で述べたように **SSH2 のみを使用する**という設定にします．[Accept protocols] のチェック欄で [SSH v1] のチェックをはずし [SSH v2] にだけチェックをいれます (図 6.10)．デフォルトでは両方にチェックが入っています．

設定を変更したら [保存] をクリックしてください．

■Access Control　限られたユーザにのみが利用できるようにするのなら，ここでユーザを限定します．[Only allow users] の [All] のチェックをはずし，右のボックスにチェックをいれ，そのうしろのボックスに許可するユーザ名を記入します．例えば hoge と

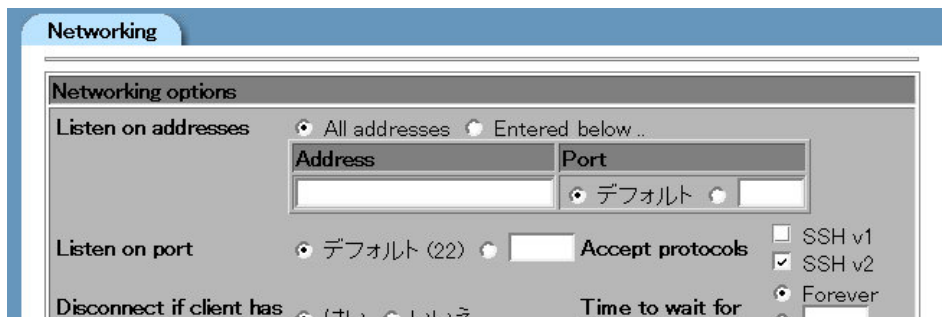



図 6.10: Networking の Accept protocols のチェック

hogehoge というユーザしか受け入れないのであれば hoge hogehoge とユーザをスペースで区切って入力します (図 6.11)．直接入力せず，ボックス右にある [...] をクリックして選択していくこともできます．[Deny users] では同様の操作で拒否したいユーザを設定します．

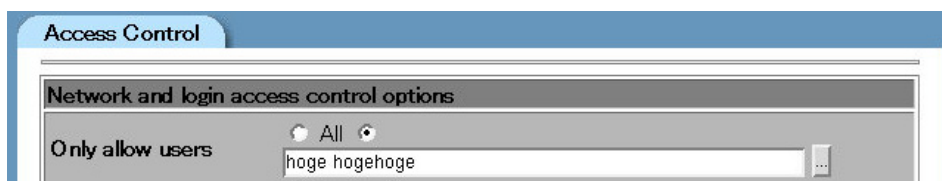



図 6.11: ユーザの限定

設定を変更したら [保存] をクリックしてください．

■設定を変更したら　設定内容のファイルは`/etc/ssh/sshd_config` に編集されて保存されます．確認のために見てみるのもよいでしょう．

ここまででは設定内容を書き換えただけです．新しい設定を反映させたサーバで起動させるさせる必要があるので，変更した設定を保存したらかならず SSH Server インデックス画面上で [Apply Changes] をクリックしましょう．これで変更後の設定が反映されます．

WU-FTP サーバ

WU-FTP という FTP サーバの設定ができます．サーバ側にアカウントがある正規ユーザだけでなく，匿名ユーザも接続できる anonymousFTP サーバにも対応しています．

まず，標準でインストールされていない場合は自分でインストールする必要があります．

■インストール　wu-ftp-xxx.rpm を手に入れて

```
[root@Linux00 hoge]#rpm -ivh wu-ftp-xxx.rpm ↵
```

としてインストールを行います．

また，anonymousFTP サーバのために anonftp-xxx.rpm も同じようにインストールし

ます．

```
[root@Linux00 hoge]#rpm -ivh anonftp-xxx.rpm ↵
```

インストールが完了したら「wu-ftpd」のデーモン[*1]を起動時に開始するように設定します．幾つか方法はありますが，どのディストリビューションでも可能な方法として「ntsysv」での設定方法を説明します．

まず，root になりシェルのコマンドラインに/usr/sbin/ntsysv と入力して実行します．ここでは起動時に実行させるデーモンが選択することができます．そこで，カーソルを「wu-ftpd」の項目に合わせて [space キー] でチェックをします．次に [Tab キー] を押して [OK] を選び終了します．もし FTP サーバをすぐに起動させたいのであればスーパーサーバである xinetd を再起動しなければなりません．これはランレベルによって多少異なります．ランレベルの確認のしかたは第 7 章を参照してください．現在のランレベルを確認したら，それに応じて次のようにデーモンを再起動します．

```
[root@Linux00 hoge]$/etc/rc5.d/S56xinetd restart ↵
```

WU-FTP がインストールがされると/home/ftp/もしくは/var/ftp/という，匿名ユーザ用のフォルダが作成されます．匿名で FTP 接続した場合はその匿名ユーザ用のディレクトリに接続されます．また正規のアカウントで接続した場合は自分のホームディレクトリに接続されます．

次に WU-FTP のアクセス制限などの必要と思われる設定を Webmin で行う方法を説明します．Webmin サーバ画面から [WU-FTP] アイコンをクリックすると WU-FTP サーバの画面 (図 6.12) が現れます．

図 6.12: WU-FTP インデックス画面

[*1] サーバのサービスを自動的に実行するプログラム

■ユーザとクラス　この項目 (図 6.13) では FTP サーバへアクセスするユーザのクラス分けやアクセス制限を設定できます．ユーザクラスには初めから [all] というクラスが定義されており，これは FTP サーバに接続してきた全ての種類のグループを [all] と言う名前のクラスにする，という意味です．このクラスを使って他の高度な制限をすることができます．ここでは他に [students] というクラスを定義しています．これは [133.87.*.*] という IP から接続してきた正規ユーザのクラスのことです．

図 6.13: ユーザとクラス

下の [拒否しない Unix ユーザと UID] と [拒否しない Unix グループと GID] に接続を許可したいユーザおよびグループを追加します．追加する際は右にある [...] のボタンをクリックしてその中から選択してください．

■制限とアクセス制御　ここ (図 6.14) ではより詳しくアクセスを制限をすることが可能です．

[アクセスを拒否] の欄では IP を指定してアクセスを拒否することができます．これを設定するときは，拒否したときに相手側に流れるエラーメッセージを指定する必要があります．これはサーバ側で流したいメッセージの文章ファイルを作ってそれを指定してください．

```
[hoge@Linux00 hoge]$echo ERROR | cat > /etc/hoge.msg
```

[同時ユーザ制限] では一度に接続できるユーザの数や時間を設定できます．ここでは先ほど定義したクラスを使って制限を行ない，メッセージファイルも指定します．図 6.14 の例では [all] というクラスは一度に 10 人までしか接続できない設定になっています．

基本的な設定は以上ですが，anonymousFTP を使う場合は十分注意して管理を行なってください．また，ここで行った設定は設定ファイル/etc/ftpaccess に書き込まれます．

図 6.14: 制限とアクセス制御

この設定ファイルを直接編集しすることで同様に設定ができます.

■接続状況の取得 FTP サーバに接続しているユーザの数や，誰が接続しているかを確認するために/usr/bin/ftpcount と/usr/bin/ftpwho の 2 つが用意されています．root になりこのコマンドを実行すれば，現在の接続状況がわかります．

```
[root@Linux00 hoge]#ftpcount ↵

Service class students            -   0 users (no maximum)
Service class all                 -   2 users (no maximum)

[root@Linux00 hoge]#ftpwho ↵

Service class students:
   -   0 users (no maximum)
Service class all:
 7503 ?        SN     0:00 ftpd: 192.xxx.xxx.xxx: anonymous/hoge@mail: IDLE
 7505 ?        S      0:00 ftpd: 192.xxx.xxx.xxx: hoge: IDLE
   -   2 users (no maximum)
```

6.4.4 ネットワーク

Webmin 画面上にある [ネットワーク] アイコンをクリックすると，ネットワークのインデックス画面が現れます (図 6.15)．ここではその中のネットワークの設定を説明します．

ネットワークの設定

ネットワークインデックス画面から [ネットワーク設定] のアイコンをクリックします．

図 6.15: ネットワーク インデックス画面

各種ネットワークの設定ができます (図 6.16).

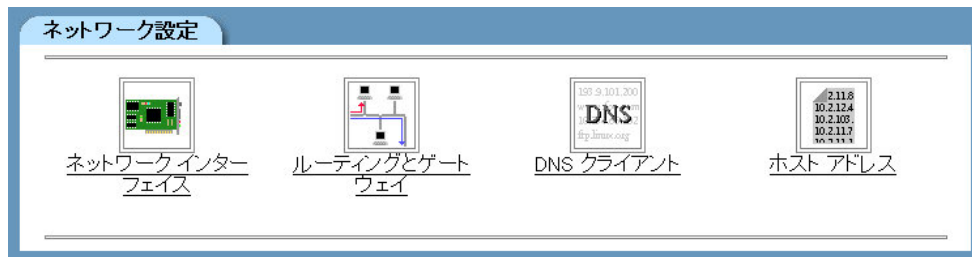



図 6.16: ネットワークの設定 モジュールインデックス画面

■ネットワークインターフェイス　ここでは，ネットワークインターフェイスの設定が出来ます (図 6.17)．設定を変更及び追加したい時は [起動時にインターフェイスをアクティブ] の項目の変更したいホスト名，または [新規インターフェースを追加] を選択します．ホスト名，IP アドレス，ネットマスク，ブロードキャストを設定し [作成] を押し，システムを再起動してください．また，設定ファイル/etc/network/interfaces を直接編集することで，同様に設定ができます．

■ルーティングとゲートウェイ　各種ルーティング設定ができます (図 6.18)．必要であれば，デフォルトルータ，デフォルトデバイス，ローカルルートなどを入力し，変更してください．設定ファイル/etc/defaultrouter を直接編集することで，同様に設定ができます．

■DNS クライアント　ここでは，DNS クライアントの設定ができます (図 6.19)．ホスト名，DNS サーバ，ドメインの検索を設定し，[保存] を押します．また，設定ファイル etc/resolv.conf などを直接編集することで，同様に設定ができます．

■ホストアドレス　ここでは，ホストアドレスの変更や，追加ができます (図 6.20)．IP アドレスをクリック，もしくは新規のホストアドレスを追加を選択します．IP アドレス，ホスト名を設定し，[作成] を押します．また，設定ファイル etc/hosts を直接編集することで，同様に設定ができます．

図 6.17: ネットワークインターフェイスの設定

図 6.18: ルーティングとゲートウェイの設定

図 6.19: DNS クライアントの設定

図 6.20: ホストアドレスの設定

第 7 章

不必要なサービスの停止

Red Hat Linux をインストールすると，初期状態で様々なサービスが起動されるように設定されます．インターネットで用いられるサーバも起動されるため，事によってはセキュリティホールとなることもあります．これら初期状態で起動されるサービスは，自分にとって不必要であれば起動しないように設定するのがセキュリティレベル向上のための第一歩と言えるでしょう．しかし，デフォルトで存在するサービスは全部で 40〜50 個強用意されています*[1]．全てのプログラムを停止させればセキュリティレベルが向上しますが，中には必ず起動しなければならないプログラムも存在するため，全て停止させてしまうと何も出来なくなってしまいます．そのため，概略だけでも各プログラムが何をするのか知っておく必要があります．この章ではランレベルの概念と，各ランレベルでの起動サービスの変更方法について，いくつかの方法を説明します．

7.1 ランレベル

Linux は UNIX 系 OS であるため，マルチユーザでの利用を前提として環境が用意されています．普段は複数のユーザが同時に利用できるような状態になっていますが，システムの基幹部の設定を変更している時は管理者以外の利用を禁止したいところです．複数のユーザが同時に利用できる状態をマルチユーザモード，管理者一人のみが利用できる状態をシングルユーザモードと呼び，マルチユーザモードにも様々な種類があるのが一般的です．Red Hat Linux では，ユーザモードが 0〜6 まで用意されており，各々のランレベルの意味は以下の通りです．

0. システム停止
1. シングルユーザモード
2. マルチユーザモード (NFS なし，ネットワークなし)
3. マルチユーザモード (ネットワークあり)
4. (未使用)
5. X Window System を用いたマルチユーザモード (ネットワークあり)

*[1] その全てが起動される訳ではありません

6. 再起動

VineLinux のインストール時で X Window System の設定に成功し，「ログインの種類」として「グラフィカル」を選択している場合，起動時のランレベルは 5 に設定されます．逆に「テキスト」を選択した場合は 3 に設定される訳です．ランレベルの段階を見るとわかるように，0 の停止段階から始まり，1 でシングルユーザモードに進化します．2 になると複数のユーザが利用できるマルチユーザモードへと進化して，3 になるとネットワークがさらに付加され，5 になるとそれにさらに X Window System が付加される，というようにランレベルが上がるごとに，それより下のランレベルに対して何か特徴が付加されるという形になっています．実際に，起動時にどのランレベルで起動する設定になっているかは/etc/inittab に記述されています．以下に/etc/inittab の内容を示します．

```
#
# inittab       This file describes how the INIT process should set up
#               the system in a certain run-level.
#
# Author:       Miquel van Smoorenburg, <miquels@drinkel.nl.mugnet.org>
#               Modified for RHS Linux by Marc Ewing and Donnie Barnes
#

# Default runlevel. The runlevels used by RHS are:
#   0 - halt (Do NOT set initdefault to this)
#   1 - Single user mode
#   2 - Multiuser, without NFS (The same as 3, if you do not have networking)
#   3 - Full multiuser mode
#   4 - unused
#   5 - X11
#   6 - reboot (Do NOT set initdefault to this)
#
id:5:initdefault:

[以下略]
```

ここで書かれている最後の行の “id:5:initdefault:” の 5 という値が起動時のランレベルを示します．この場合は X Window System が起動したマルチユーザモードとして起動することを表しています．次のセクションでは各ランレベルごとの起動サービスの設定を行いますが，全てのランレベルについて設定する必要はありません．自分が主として使うランレベルについてのみ設定を行いましょう．

7.2　起動サービスの設定

起動サービスの設定は，X Window System 上で動く GUI アプリケーションによる設定と，コンソール上で動く GUI アプリケーションによる設定，そして手作業による設定があります．当初は GUI アプリケーションによる設定で構いませんが，慣れるに従って，GUI アプリケーションが実際のファイルに対してどのような変更を加えているのかを知るべきです．手作業で実際に起動サービスの変更を行ってみると，実に簡単なことで変更

が行えることを知ることができるでしょう．

GUI での設定するためにはコマンドラインから redhat-config-services を実行するか，あるいは画面左下にある Red Hat のメニューアイコンをクリックして [サーバ設定] → [サービス] と指定するかのどちらかで実行することができます (図 7.1)．どちらで行うにしても root 権限が必要です．

図 7.1: メニューアイコンからサービスへ

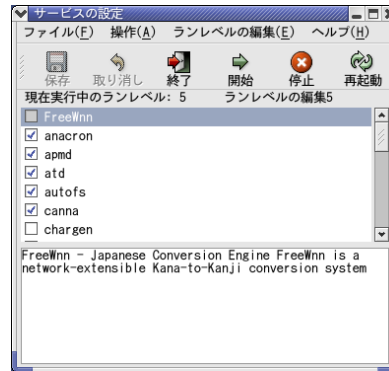



図 7.2: redhat-config-services

redhat-config-services では runleve3〜5 までについて編集することが可能であり，メニューにある [ランレベルの編集] から指定することができます．チェックボックスを ON/OFF することで各々のスクリプトを起動するかどうかを指定することができ，また，各スクリプトを実際に開始・停止・再起動させることもアイコンから可能です．また選択したスクリプトに関する簡単な記述が下部に記述されるので，どのような内容であるかをざっと知ることができるでしょう．

また，redhat-config-services が行う作業をターミナルなど，コマンドライン上で自力で行う場合，/etc/rc.d ディレクトリへと移動しましょう．ここには rc3.d, rc4.d, rc5.d といったディレクトリが存在し，それぞれこのディレクトリについている数字がランレベルに対応します．ランレベル 5 について編集したい場合は rc5.d ディレクトリに入ります．

そこで ls コマンドを実行するとわかるように，このディレクトリには “K” で始まるファイルと “S” で始まるファイルの二種類があります．K で始まると無効で，S で始まると有効になるという極めて単純なルールによって起動する/しないが決定されます．また，実はこれらはファイルではなく，実体のないシンボリックリンクであり，/etc/init.d にあるスクリプトの実体を指し示しているだけのものです．

このディレクトリにあるこれらのシンボリックリンクは名前からその機能が類推されますが，有効にしたい場合は，名前の先頭を “S” にする必要があります．逆に無効にしたい場合は “K” にする必要があります．例えば S80sendmail というファイルは，sendmail スクリプトが起動時に実行されるという事を意味しますが，これを無効にしたい場合は

```
[reo@Linux00 rc5.d]# mv S80sendmail K80sendmail ↵
```

とします．これはシステムの根幹に関わることですので，root 権限がないと出来ません．

このようにして起動時に実行されるスクリプトの有効・無効を設定させることが出来ますが，各スクリプトを有効にして良いのか，無効にするべきなのか，判断が難しいかと思われます．そこで 40 個強ある起動スクリプト について簡単に説明し，クライアントとして利用する場合における有効・無効の指針について述べることにしましょう．

1. FreeWnn
   かな漢字変換プロセッサ FreeWnn を起動します．FreeWnn を使う人は**有効にしましょう**．

2. anacron
   定期的にプログラムを実行する cron というプログラムがありますが，24 時間常時稼働していない Linux マシンの場合，cron で実行される予定時刻に Linux が起動していないと，そのプログラムは次回まで実行が持ち越されてしまいます．毎日実行するプログラムなら，次回まで持ち越されてもそれほど問題がないかもしれませんが，一ヶ月に一度という実行頻度のプログラムの場合，一ヶ月後まで持ち越されてしまうのは問題があるかもしれません．anacron は，起動時にそういったスケジュールをチェックして，起動されなかったプログラムを一括処理するプログラムです．**これは必ず有効にしておきましょう**．

3. apmd
   電源の管理規格である APM に対応したマシンの場合，apmd により具体的に電源管理を行います．例えばうっかり電源ボタンを押してもシャットダウンしないようになどといったサポートがそれに当たります．しかしマシンによっては，この APM への対応が故に起動しないという場合も有り得るので，APM が原因で起動しない場合は無効にしておきましょう．特に問題ない場合は有効にしておくのが望ましいです．

4. atd
   指定時間にコマンドを実行する at コマンドがありますが，これを実行するのに必要なサービスです．at コマンドは何かと重宝するので**これは必ず有効にしておきましょう**．

5. autofs
   自動的にファイルシステムをマウントする仕組みが autofs により有効になります．CD などが入っていた場合，自動的にマウントされます．必須という訳ではないですが，あると重宝するので**有効にしておいた方が良いでしょう**

6. canna
日本語入力システム「かんな」を利用する時には必須のサービスです。VineLinux の FTP 版[*2]などでは，かな漢字変換システムとして「うんぬ」と「かんな」が用意されているが，かんなを使っている人は絶対に**有効にしなければいけません**.

7. crond
前述の cron を実行するのに必要です．cron も何かと重宝するので**これは必ず有効にしておいた方が良いです**.

8. firstboot
初回起動時に実行されるスクリプト．この説明の通り初回起動時以外に必要ありません．**無効にしておきましょう**.

9. functions
ほとんど全てのシェルスクリプトで用いられる関数がここで記述されています．そのため，これは**必ず有効にしなければなりません**.

10. gpm
コンソール上でマウスの利用をサポートする場合に有効にします．コンソールでマウスを使っても仕方がないという人は**無効にして構わない**でしょう.

11. halt
これはランレベルを 0 や 6 にする時，即ち停止状態や再起動するときに実行されるスクリプトです．起動時にこれを実行すると，起動してまもなく停止状態になりますので**絶対に無効にして下さい．**

12. iptables
パケットフィルタリングの仕組みを有効にします．**有効にしましょう**.

13. irda
IrDA (InfraRed Data Association) による赤外線通信機能を有効にします．実際のところ IrDA を利用することがない人は**無効にして問題ありません**．が，利用する人は有効にしたほうが良いでしょう.

14. ISDN
ADSL にとって代わられた高速回線のことですが，HINES に関係ない上，おそらく日本ではこの設定を使えないのではないかと思われます．**無効にしましょう**.

15. keytable
各言語用のキーボードの設定を行います．これを有効にしないと，キーボードの刻印とは異なる文字が画面に表示されて非常に苦労すると思われますので，必ず有効

*2 雑誌付録の CD-ROM に収録されているものがそれに当たる

にしましょう．

16. kdcrotate
Kerberos 認証に必要とされる機能．Kerberos 認証を使っていないならば**無効にしてしまいましょう**．

17. killall
不必要としているサービスにも関わらず起動しているものをすべて止めるためのスクリプトです．/etc/init.d ディレクトリにこのスクリプトは存在しますが，恐らく ntsysv といった設定ツールには表示されないです．

18. kudzu
新規ハードウェア検出ツールです．Windows で言うならばプラグアンドプレイウィザードのようなものでしょうか．何かと重宝しますので**有効にしておきましょう**．

19. lpd
印刷サービス．プリンタを利用する際の定番です．プリンタを使わないという場合はほとんど考えられないでしょうから，**有効にしておきましょう**．

20. netfs
/etc/fstab にはどのデバイスをどこにマウントするかという情報が記述されていますが，このファイルに記述されているネットワークデバイスをマウントしてくれるのが netfs です．NFS を利用している時は必需品ですが，そうでない時は必要ありません．マシンの台数が増えてくると，NFS は非常に有用となりますし，忘れないうちに**有効にしておくべき**かもしれません．

21. network
ネットワークの設定です．これを有効にしておかないとインターネットへの接続もままなりません．ネットワークを利用するなら**必ず有効にしましょう**．

22. nfs
NFS サーバのデーモンを起動します．自分が NFS サーバにならないのであれば起動する必要もありません．シンプルな 1 クライアントとしては**無効で構わない**かもしれません．

23. nfslock
NFS サーバのユーティリティです．NFS サーバを有効にしているならば同時に必要となりますが，そうでないならば同時に不必要です．**nfs と同じ設定にしておくべき**でしょう．

24. nscd

NIS や LDAP などを高速化してくれるデーモンを起動します．NIS や LDAP を利用していないのであれば**無効にしておくべき**でしょう．

25. ntpd
    NTP (Network Time Protocol) のサーバです．時刻を極めて正確に合わせてくれるため，几帳面な人には必須です．そうでない人にとっても何かと有用ですから，ntpd の設定を適切に行った後，**有効にしておきましょう**．

26. pcmcia
    PCMCIA を司るデーモンを起動します．ノート PC など PC カードを利用するマシンにおいては必要ですが，そうでないならば不必要です．大雑把に**ノート PC 利用時に必要**としておきます．

27. portmap
    portmapper を起動します．portmapper は NIS サーバや NFS サーバを利用する時に必要となります．これらのサーバを起動していないならば**無効で構いません**．

28. postfix
    強力なメールサーバである postfix を起動します．ローカルでメールサーバを運用しないのであれば**無効にしましょう**．

29. random
    乱数を発生させます．様々なアプリケーションはこれを利用している場合がありますので，**必ず有効にしましょう**．

30. rawdevices
    raw device を block device に割り当てるという機能を持ちます．詳しい機能については深く考えず，これは**有効にしましょう．**

31. rhnsd
    Red Hat Network へ接続して定期的にアップデートをチェックしてくれるデーモンを起動する．**有効にしておく**．

32. saslauthd
    次に説明する sendmail と連動して SMTP 認証を行うためのデーモンを起動します．ローカルでメールサーバを運用しないのであれば**無効にしましょう**．

33. sendmail
    メールサーバである sendmail を起動します．ローカルでメールサーバを運用しないのであれば**無効にしましょう**．

34. single
    /etc/init.d ディレクトリには存在するものの，自動設定ツールでは現れないであ

ろうスクリプト．シングルユーザモードで起動した時のみ実行されます．

35. snmp*

    snmp で始まるネットワークモニタリングを有効にします．ネットワークを詳細に渡って監視できる有益なツールですが，必ずしも必要という訳でもありません．必要性が感じられない人は**無効にしましょう**.

36. sshd

    SSH サーバを起動します．SSH はセキュリティのためにも利便性のためにも非常に有益です．是非，適切な設定を行って**有効にしましょう**.

37. syslog

    ログ記録サービスである syslog を有効にします．様々なログから非常に有益な情報を数多く得る事ができますので**必ず有効にしましょう**.

38. xfs

    X Font Server を起動します．X 上でフォントを利用する際に必要となりますので**必ず有効にして下さい**.

39. xinetd

    インターネットスーパーサーバを起動します．これは非常に重要なので**必ず有効にしておきましょう**.

40. ypbind

    NIS クライアントを起動します NIS を利用しないなら**無効にしましょう**.

おわりに

北海道大学では，現在，学術情報委員会の下で情報セキュリティポリシーが策定され，その実施に向けての準備が進められています．情報セキュリティポリシーとは，組織が有する情報資産を破壊から守り，情報の不正な利用を阻止するための方策を総合的，体系的かつ具体的にまとめたものです．

このポリシーの中では，情報セキュリティ対策のために，3 階層のピラミッド構造を有する全学的な組織が定められています．上位層は最高情報セキュリティ責任者（総長あるいは副学長）とその意思決定を補佐する情報セキュリティ委員会からなり，統括的な管理レベルに対応します．一方，中位層は実務レベルに対応する情報システム管理部会からなり，緊急のインシデント対応など実務面から最高情報セキュリティ責任者を補佐します．個々の情報機器（パソコンなど）のシステム管理者および利用者は下位層に属します．本学におけるパソコン普及の実状から考えて，ほとんど全ての教官あるいは職員がシステム管理者に該当すると思われます．

ここで注意しておきたいことは，個々の情報機器に関して，そのセキュリティを維持管理する責任と義務を有するのは，その情報機器のシステム管理者自身であるということが，本学情報セキュリティポリシーに明記されていることです．さらに，上位層からのトップダウン的な周知事項に限らず，システム管理者は自ら率先してセキュリティ情報の収集に注意し，改善に努めなければならないことも述べられています．

すなわち，情報セキュリティは他人任せではなく，自助努力を伴った各人の責任ある対応が求められています．過保護な無菌室状態に創造性はありません．自然界の生物と同じように，免疫力すなわち自ら学ぶ力を養うことが肝要です．ネットワーク社会における北海道大学のプレゼンスは，まさに本学構成員一人一人のそのような自覚にかかっています．あなたのパソコンを守るということは，結局のところ，我が北海道大学のプレステージを守ることに他ならないのです．

本学情報セキュリティポリシーはその実施手順が策定され，体制が整い次第，本格的な運用に移っていくことでしょう．一般に，情報セキュリティポリシーの階層構造から言うと，個人向けセキュリティ対策マニュアルは，ポリシーの実施手順の一部に対応します．本セキュリティマニュアルが，今後情報セキュリティ委員会によって策定される予定のポリシー実施手順や個人マニュアルを考える上での一つのモデルとなれば幸いです．

本セキュリティマニュアルは，平成 14 年度プロジェクト研究（情報基盤センターの機能開発）「利用者向け情報セキュリティ対策マニュアルの作成および方法論に関する調査研究」の一環として作成いたしました．特に，工学研究科システム情報工学専攻および電子情報工学専攻の大学院生から多大の協力を得ました．感謝の意味を込めて，名前を紹介いたします．

柏崎 礼生君， 岸辺 知也君， 槇 康仁君， 和田 弘重君，
東海林 智也君， 扇谷 篤志君， 佐藤 祐介君， 島村 徹平君， 弘 新太郎君

研究組織：
水田 正弘（情報メディア教育研究総合センター）（研究代表者, Windows 班責任者）
高井 昌彰（大型計算機センター） （Linux 班責任者）
南 弘征（情報メディア教育研究総合センター）
小宮 由里子（情報メディア教育研究総合センター）